
ARMY FIELD MANUAL VOLUME 1 COMBINED ARMS OPERATIONS

PART 4

COUNTERSURVEILLANCE, OPSEC & DECEPTION

This publication supersedes
AC 70753 *Unit Battlefield Countersurveillance* dated June 1994 and
AC 71359 (Pt 5) *Deception in War* dated 1990

1999

Copyright This work is Crown copyright and the intellectual property rights for this publication belong exclusively to the Ministry of Defence (MOD). No material or information contained in this publication should be reproduced, stored in a retrieval system or transmitted in any form outside MOD establishments except as authorised by both the sponsor and the MOD where appropriate.

Security This document is issued for the information of such persons who need to know its contents in the course of their official duties. Any person finding this document should hand it into a British Forces unit or to a British police station for its safe return to the MINISTRY OF DEFENCE, D MOD SY, LONDON SW1A 2HB, with particulars of how and where found. THE UNAUTHORIZED RETENTION OR DESTRUCTION OF THIS DOCUMENT COULD BE AN OFFENCE UNDER THE OFFICIAL SECRETS ACTS OF 1911-1989.

Authority This publication is issued under the overall direction of the CGS . It is an MOD Approved Code of Practice (ACOP). Where issues of health and safety are concerned it takes into account the provisions of the Health & Safety at Work Act 1974.

Status The contents provide clear military information concerning the most up to date experience and best practice available for commanders and troops to use in their operations and training. If you are prosecuted for a breach of health and safety law, and it is proved that you have not followed the relevant provisions of the ACOP, a court may find you criminally liable unless you can show that you have complied with the requirements of health and safety legislation since it is a breach of this legislation which renders a person criminally liable. Breaches or omissions of the ACOP could result in disciplinary action under the provisions of the Army Act.

Amendment

Amendment No	Date	Amendment No	Date

Distribution As directed by DGD&D, LW1 who is the sponsor and to whom comments and queries concerning this publication should be addressed.

“Always mystify, mislead and surprise the enemy.”

Thomas “Stonewall” Jackson

PREFACE

1. This publication addresses Countersurveillance, Operations Security (OPSEC) and Deception. These three subjects are distinct disciplines in their own right, but have the same aim, which is to deny or distort the enemy's situational awareness; in other words, to prevent him from locating and identifying our true intentions, forces involved, locations, objectives, timescales and tactics.
2. Countersurveillance is a fundamental part of battlefield discipline, the importance of which cannot be over-emphasised. It is an art which has to be practised at every opportunity because it can be a vital factor in achieving success on the battlefield. The key to countersurveillance is a knowledge of the threat. The introduction of modern, technologically advanced battlefield surveillance sensors has significantly increased the threat of being seen and engaged by an enemy. The battlefield is becoming increasingly transparent.
3. OPSEC recognises that, at unit level and above, it is impossible to conceal all military activities, so instead, it aims to deny the enemy enough information to prevent him ascertaining the details of that activity - so although the enemy know where friendly troops are located, he cannot determine their exact positions or intentions. It is planned and co-ordinated at unit level and above, although its implementation is the responsibility of all force members.
4. Deception takes this process a stage further, and aims to give the enemy a false picture of friendly activities - thereby causing him to take an action which can be exploited. It is normally a formation responsibility, but can be used at a lower level.
5. The three disciplines are thus complimentary: countersurveillance is essential to the OPSEC plan for it to be effective; and deception requires both effective countersurveillance and an integral OPSEC plan to conceal those real activities that could compromise the false picture being portrayed. The aim of this publication is to serve as a guide to those measures that should be employed to countersurveillance by the enemy, improve OPSEC and encourage the effective use of deception measures.
6. AFM Vol 1 Part 3 *Surveillance, Target Acquisition and Reconnaissance* describes the process and procedures of these associated functions and this publication is complementary to it. Both are necessary to obtain a full and overall understanding of these important battlefield functions.

CONTENTS

PREFACE

iii

PART A - COUNTERSURVEILLANCE

CHAPTER 1 - COUNTERSURVEILLANCE

Section

1	Principles of Countersurveillance	1 - 1
2	Identifying the Threat	1 - 2
3.	Countersurveillance Control Measures	1 - 3

Annexes:

A	Countersurveillance Control Measures	1 - A - 1
B	Equipments Covered by Control Measures	1 - B - 1
C.	Camouflage and Concealment Aide Memoire	1 - C - 1

CHAPTER 2 - CAMOUFLAGE

Section

1	Introduction	2 - 1
2	Factors of Detection	2 - 1
3	Principles of Camouflage	2 - 3

CHAPTER 3 - SPECIFIC ASPECTS OF COUNTERSURVEILLANCE

Section

1	The Soldier	3 - 1
2	Defended Localities	3 - 1
3	Armour	3 - 3
4	Artillery	3 - 7
5	Engineers	3 - 12
6	Communications	3 - 16
7	Helicopters	3 - 19
8	Vehicle and Road Movement	3 - 21
9	Stores and Installations	3 - 23

CHAPTER 4 - CAMOUFLAGE IN SPECIFIC ENVIRONMENTS

Section

1	Cold Weather Conditions	4 - 1
2	Desert Environments	4 - 4
3	Mountain Environments	4 - 5
4	Jungle Environments	4 - 6

CHAPTER 5 - COUNTERSURVEILLANCE TRAINING AT UNIT LEVEL

Section

1	Training	5 - 1
2	Preparation and Self-Help	5 - 2
3	Equipment	5 - 2
4.	The STANOC Centre	5 - 5

PART B - OPSEC

CHAPTER 1 - BACKGROUND TO OPSEC

Section

1.	The Operational Environment	1 - 1
2.	Concept of OPSEC	1 - 2

CHAPTER 2 - THE PROCESS AND EVALUATION OF OPSEC

Section

1.	Principles of OPSEC	2 - 1
2.	The OPSEC Process	2 - 2

Annexes:

A.	Examples of Essential Elements of Friendly Information	2 - A - 1
B.	Format for the OPSEC Estimate	2 - B - 1

CHAPTER 3 - OPSEC MEASURES

Section

1.	General Points	3 - 1
2.	Defensive Measures	3 - 1
3.	Active Measures	3 - 2
4.	Other Measures	3 - 3

Annex:

A. Useful OPSEC Measures	3 - A - 1
--------------------------	-----------

CHAPTER 4 - COMMAND AND CONTROL OF OPSEC

Section

1 Responsibilities	4 - 1
2 Intelligence Requirements of OPSEC	4 - 4

PART C - DECEPTION

CHAPTER 1 - BACKGROUND TO DECEPTION

Section

1 The Operational Environment	1 - 1
2 The Purpose of Deception	1 - 2
3 Principles of Deception	1 - 3

CHAPTER 2 - THE DECEPTION TARGET

Section

1 The Enemy	2 - 1
2 The Implications for Deception	2 - 4

CHAPTER 3 - DECEPTION TECHNIQUES

Section

1 The Approach	3 - 1
2 Deception Techniques	3 - 2
3 Types of Deception Activity	3 - 3

Annex:

A. Examples of Battlefield Deception and Supporting Measures	3 - A - 1
--	-----------

CHAPTER 4 - THE DECEPTION PROCESS

Section

1 General Points	4 - 1
2 Mission Analysis	4 - 2
3 Evaluation of Factors	4 - 3
4 Consideration of COA	4 - 6

5	The Commander's Decision	4 - 7
6.	Deception Planning	4 - 7
7.	The Conduct of Deception Operations	4 - 8
8.	Other Considerations	4 - 10
9.	Command and Control of Deception	4 - 10

Annex:

A.	Short Format for the Deception Estimate	4 - A - 1
B.	Intelligence Requirements for Deception	4 - B - 1
C.	Requirements for Dummy Locations	4 - C - 1
D.	Deception Planning Worksheet	4 - D - 1

CHAPTER 5 - DECEPTION IN OPERATIONS OTHER THAN WAR (OOTW)

Section

1	General	5 - 1
2	The Deception Target	5 - 1
3	Deception Techniques	5 - 2

CHAPTER 6 - COUNTERING DECEPTION

Section

1	The Possibility of Being Deceived	6 - 1
2	Countermeasures	6 - 1

Annexes:

A.	Maskirovka	6 - A - 1
B.	Intelligence Requirements for Counter Deception	6 - B - 1

PART D - HISTORICAL SUPPLEMENT

CHAPTER 1 - OPERATION BERTRAM. WESTERN DESERT 1942

CHAPTER 2 - OPERATION DESERT SABRE. THE GULF 1991

CHAPTER 3 - THE REGROUPING OF 3 GUARDS TANK ARMY. UKRAINE 1943

CHAPTER 4 - EXAMPLES OF PARTICULAR TECHNIQUES

OPSEC	The Ardennes Offensive, Europe 1944 Dien Bieu Phu, 1953/54
Deception	Marlborough's March to the Danube 1704 Yom Kippur, Oct 1973 Falkland Islands May 1982

PART A

COUNTERSURVEILLANCE

CHAPTER 1

COUNTERSURVEILLANCE

SECTION 1 - PRINCIPLES OF COUNTERSURVEILLANCE

Introduction

1. There are many different types of surveillance sensor used to detect and identify targets on the battlefield. These are described in detail in AFM Vol 1 Part 3, *Surveillance, Target Acquisition and Reconnaissance*. A knowledge of the systems in use will aid countersurveillance planning and practice. Nations, including the UK, devote considerable resources to the development of new and improved sensors in order to upgrade their surveillance capabilities; the threat is continually evolving, and has to be reviewed frequently.
2. No matter how technically advanced the equipment is or how well trained the operator, they both have their limitations. These limitations need to be fully exploited to counteract an enemy's surveillance plan. To be effective, any information gained has to be timely. It can thus be almost as effective to delay the acquisition of information or to prolong the time it takes to process it as it is to completely deny that information to the enemy.
3. A countersurveillance plan is designed to prevent an enemy acquiring information from the variety of surveillance, target acquisition and reconnaissance (STAR) resources at his disposal¹. A good plan can also cast doubt upon the effectiveness of his sensors. The countersurveillance plan is also an integral part of the Operations Security (OPSEC) process.

Principles of Countersurveillance

4. There are 6 principles of countersurveillance. These are:
 - a. To be aware of the enemy surveillance and target acquisition threat.
 - b. To avoid detection by the enemy's routine surveillance.
 - c. To blend with the environment.
 - d. To minimise movement and transmissions.
 - e. To use deception correctly.
 - f. To treat night as day.

1. See AC 71473 *Land Component Handbook* Pt 1 Serials 106 and 212A.

SECTION 2 - IDENTIFYING THE THREAT

5. ***Countersurveillance and Intelligence Preparation of the Battlefield (IPB).*** The more that is known about the threat the easier it is to counter. Surveillance sensors are unlikely to be deployed in such numbers that they will be able to cover the entire battlefield all of the time. The enemy surveillance threat can be determined from the IPB process (see AFM Vol 1 Part 8 *Command and Staff Procedures*):
 - a. *Step 1 – Battlefield Area Evaluation.* This will identify potential mobility corridors and avenues of approach. The surveillance threat will be greater in these areas, as the enemy is likely to concentrate his STAR resources there. Terrain and climatic factors will also be considered, allowing potential dead ground and weather conditions which will affect the performance of enemy STAR systems to be identified.
 - b. *Step 2 – Threat Evaluation.* Basic intelligence data will identify the enemy's STAR capabilities; their types and performance characteristics. This information is integrated with his assessed doctrinal Courses of Action (COA) and used to deduce his doctrinal surveillance plan.
 - c. *Step 3 – Threat Integration.* The results of the battlefield area evaluation and threat evaluation are integrated to identify how the enemy's doctrine will be shaped by the battlefield environment and turned into practice. This in turn will enable his probable STAR deployment and areas of coverage to be identified. These can be displayed graphically. It should be borne in mind that the enemy will have conducted a similar evaluation and will doubtless deploy, for instance, ground recce patrols to cover gaps left by other technical STAR assets. It will, however, guide the development of the countersurveillance plan and enable the commander to prioritise his unit's countersurveillance measures.
6. ***The Overhead Surveillance Threat.*** The overhead (satellite) imagery surveillance threat has increased significantly over the last few years. Once restricted to the US and Former Soviet Union, a number of nations now possess or have access to imagery satellites, operating in the visible, infrared and radar bands of the electromagnetic spectrum. In addition, a number of commercial concerns are planning to operate imagery satellites in the near future. Imagery from these satellites will be available on the open market. The resolution of much of the imagery that can currently be purchased is of limited use for detailed military analysis but this will change when sub 1 metre resolution commercial systems become operational. Countermeasures against satellite-borne surveillance systems are the same as those for conventional aerial reconnaissance and surveillance. Commanders must therefore assume that they could be subject to satellite surveillance and plan accordingly. Information on the position of operational imagery satellites, and thus their ground "windows", is available from the UK Satellite Warning Service through formation HQs and this information should be taken into consideration when planning operations.
7. The precautions to take against the STAR threat are known as Emission Control (EMCON). EMCON SOPs are issued at all levels of command.

SECTION 3 - COUNTERSURVEILLANCE CONTROL MEASURES

8. **General Points.** Measures taken by commanders as precautions against the STAR threat include control of the use of the following:
 - a. Communications equipment by the imposition of radio silence either on its own or as part of electronic silence (COMMS EMCON).
 - b. Non-communications equipments such as radars, lasers, navigation aids, IFF, homing beacons, sondes, tellurometers, active IR and radio data links associated with sound ranging, BUT less white light, by the imposition of electronic silence (NON COMMS EMCON).
 - c. White light for target acquisition.
 - d. Direct and indirect fire.
 - e. Vehicle lights.
 - f. Noise and movement by personnel and vehicles.
 - g. Non-operational heat sources, including cookers and running engines to keep vehicles warm.
9. **Electronic Silence.** Electronic silence applies to all electronic equipment. It should be remembered that radios, even when set to receive only, cause emissions which can be detected by enemy Electronic Support Measures (ESM). A total silence on all equipments will be the exception; a series of control measures is therefore necessary. These are recorded in both the *Land Component Handbook* and TAM Pt 3. It has to be understood that the measures are quite separate and not necessarily sequential. The control measures may be imposed by a commander at any level and will initially be included in the Operation Order.
10. **Other Measures.** Other measures to counter enemy surveillance include:
 - a. *Blending With the Environment.* The aim of camouflage is to conceal a target so that it cannot be distinguished from its surroundings. To disguise the presence of a target requires wise use of the surroundings and knowledge of the capabilities of the enemy's surveillance sensors.
 - b. *Minimising Movement.* Movement is one of the major factors in detecting a target in any type of surrounding. Movement attracts the attention of optical sensors and Doppler (MTI) radars. Movement also produces a number of side effects such as tracks, hot engines and dust, all of which can be detected. A countersurveillance plan must ensure that all movement is kept to a minimum. Comparatively fast, regular movement will be detected more easily than slow, irregular movement.

- c. *Unit-Level Electronic Protective Measures (EPM).* EPM includes active and passive measures designed to prevent or minimise detection by ESM. These measures should be an integral part of unit communication drills.
- d. *Treating Night as Day.* Many modern sensors operate as well by night as they do by day. They are also capable of operating through smoke and periods of poor visibility caused by adverse weather conditions such as rain, mist and fog. Therefore, night does not give protection from surveillance. It must be assumed that the enemy will use passive surveillance devices at night, so countersurveillance measures must be applied at night in the same way as they are by day.
- e. *Counter Reconnaissance.* Counter reconnaissance includes all active measures taken throughout the area of operations. Its goal is to detect, engage, deny, defeat or destroy enemy reconnaissance and surveillance assets to prevent them observing friendly activities, defining positions or taking direct action against a unit or force. All enemy reconnaissance encountered should be destroyed unless ordered otherwise, and clear orders for the engagement of enemy reconnaissance should be promulgated.
- f. *Smoke.* Screening smoke is effective against sensors operating in the visual part of the spectrum. Thermal imagers can only be countered by multi-spectral smoke, which is not currently on general issue. Smoke can only be used under favourable weather conditions, and is only effective for a limited period, but can be used to conceal particular phases of an operation. However, the use of smoke will alert the enemy to the fact that something is happening. Smoke is best used to cover actions that will impact upon the enemy almost immediately, thus giving him insufficient time to identify the activity covered by the smoke and react to it.
- g. *Deception.* When no practicable measures exist to counter a particular STAR threat, the use of tactical deception should be considered. Deception includes the art of making the enemy believe that false information is true. A well-planned and executed deception plan will weaken the enemy's strategic, operational and tactical plans. It can also have considerable psychological impact. All deception plans need to be well planned and co-ordinated at the highest level of command involved in the operation to avoid creating 'own goals'. Part C of this volume deals with deception in more detail.

Aides Memoire

- 11. Countersurveillance Control Measures, the equipments covered by these control measures and Camouflage and Concealment Aides Memoire are shown in Annexes A, B and C to this Chapter.

COUNTERSURVEILLANCE CONTROL MEASURES

MEASURES	RADIO	NON COMMUNICATIONS EQUIPMENT	WHITE LIGHT ILLUMINATION	FIRE CONTROL	VEHICLE LIGHTS	NOISE/HEAT/ MOVEMENT SOURCES
PREFIX	"A"	"B"	"C"	"D"	"E"	"F"
1	SILENCE IMPOSED All radio and radio relay transmitters to be switched off. Receivers to remain on and manned.	Total silence. No electronic emission is to take place, even for testing.	No white light to be used. Surveillance to be by passive means only.	No firing without permission of commander who imposed measure.	No light of any sort including IR.	Total silence. No engines to be run. No heat sources. No movement of personnel/vehicles.
2	For "BREAKING RADIO SILENCE" (See Para 7 to AFSOP 602 and specific theatre emcon rules).	Minimum essential testing only. Silence may be broken for specific engagements, missions or tasks, but must be reimposed immediately afterwards.	Use of white light for emergency engagements but measure 1 must be reimposed afterwards.	Firing only in self defence by individuals/units coming under direct enemy fire. No other fire except on authority of commander who imposed measure.	Convoy light only. No IR.	Minimum essential running of engines/ generators. Minimum use of heat sources and movement of personnel/vehicles.

3	SILENCE LIFTED All radio and radio relay transmitters and receivers to be on and manned. Normal radio procedures.	As for measure 2 until first engagement, mission or task after which silence is lifted for that weapon or equipment.	Normal use.	All weapons subject to normal fire control.	Side and convoy lights. (Commanders must specify if IR may be used).	Normal use of engines/ generators/heat sources, vehicles/personnel movement, to maintain full operational capability.
4			SILENCE LIFTED			

Note: These measures are separate and non-sequential.

Appendix:

1. Equipment Covered - Likely Measures and Remarks.

EQUIPMENTS COVERED BY CONTROL MEASURES

"A"	"B"	"C"	"D"	"E"	"F"
1. Radio 1 or 3 2. Radio relay 1 or 3.	1. <u>Formation Equipment.</u> a. AD radar 1, 2, 3. b. Weapon locating radar 1, 2, 3. c. AMET radar and radio sondes 1, 2. d. DRONE homing beacon 1, 2. e. Sound ranging 1, 2, 3. f. Tellurometer 1, 2. g. RADALT, TANS. MINITANS 1, 2. h. IFF 1,2.	1. Tank searchlight. 2. Handheld flares. 3. 51mm and 81mm mortar illumination. 4. 105mm and 155mm artillery illumination. 5. Movement Light (AFSOP 603).	All	All	1. Engines. 2. Generators. 3. Burners. 4. Cookers. 5. Heaters. 6. Oxy-acetylene. 7. Movement of personnel and vehicles.
	2. <u>Unit Equipment.</u> a. Ground surveillance radar 1, 2, 3. b. Active IR 1, 2. c. IRIS 1, 2, 3. d. Lasers 1, 2, 3.	Note: Commanders must specify whether trip flares are to be set.		Notes: 1. Brake lights to be disconnected in all cases. 2. For road movement convoy lights see AFSOP 801.	Note: Usually ordered at unit level.

CAMOUFLAGE AND CONCEALMENT AIDE MEMOIRE

SERIAL	THREAT			ACTION
	WAVEBAND	FROM	ENEMY EQPT	
(a)	(b)	(c)	(d)	(e)
1.	Visible	Eyeball by optics and TV	All vehicles, dismounted infantry, aircraft including helicopters	Reduce shape, shine, shadow and movement, Match colour, pattern and
		Aerial Imagery	Satellites and aircraft including Unmanned Aerial Vehicles (UAV)	Siting and track discipline, natural and artificial camouflage, eg nets (Arctic, Desert or Woodland) or Urban Camouflage Material (UCM).
		II	Weapon sights and NODs (2)	
	Visible/Near IR (1)	Low Light TV	AFVs, aircraft including helicopters and RPVs	Treat night as day.
2.	Near IR (Active)	IR Sources IR Viewers	Illuminators, weapon sights and driving aids.	Same as Serial 1. Treat night as day. Minimise light sources. Minimise active IR sources.
	(Passive)	False Colour Imagery	Aircraft	In woods use IR reflectant paint and nets. In urban areas vehicles and personnel should ideally be sited inside buildings; failing this use UCM or local materials to cover IR reflectant paint and blend with surroundings.
3.	Far IR (Passive)	Thermal	Viewers, sights aircraft and RPVs; IR linescan. Aircraft and helicopters: Forward Looking IR.	Disguise or hide heat signatures by improvised screening; minimising/heat generator, using thick cover, preferably buildings; using normal camouflage and dead ground in rural areas. Using thermal camouflage material under camouflage nets.
4.	Radar (Active)	Ground Surveillance Radar	Dismounted and vehicle mounted.	Use dead ground and minimise movement.
		Sideways Looking Airborne Radar	Reconnaissance Aircraft	

Notes:

1. II and LLTV sensors operate in the visible and Near IR part of the EM spectrum. 2. NOD - Night Observation Device.

CHAPTER 2

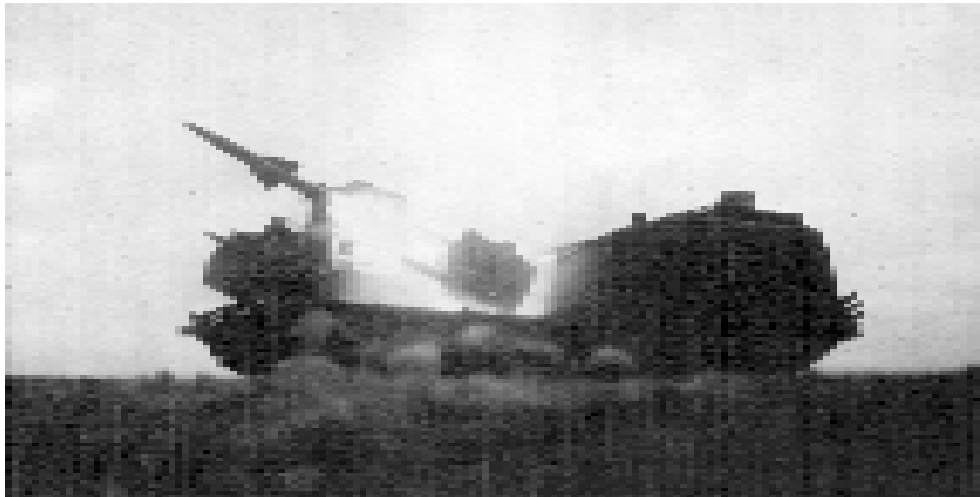
CAMOUFLAGE

SECTION 1 - INTRODUCTION

1. Camouflage is defined as “the use of natural or artificial material on personnel, objects or tactical positions with the aim of confusing, misleading or evading the enemy”.¹
2. Camouflage is the process of making a person or object blend with its background. Where circumstances make it impossible to make a target completely undetectable, we must make certain that it is not detected by routine surveillance. This will avoid encouraging the enemy to use more discriminating surveillance devices in our area.
3. Despite the capabilities of surveillance sensors, it is still expected that 75% of the information gained on the battlefield (excluding EW) will be gained in the visual band of the EMS. Therefore camouflage is mainly directed against sensors operating in the visible and IR bands. Camouflage will also assist in the protection from detection by sensors operating in the other bands of the EMS.

SECTION 2 - FACTORS OF DETECTION

4. **General.** Effective camouflage can only be judged when seen from the enemy's perspective. The enemy continuously looks for indications of a target on the battlefield. These indicators are the factors of detection that characterise a target.
5. **Shape.** The natural rural background against which most military equipment is normally viewed is random, rounded and variegated. Military equipment normally has hard, regular and uniform lines. Camouflage nets when erected often take on smooth curved lines between their support points. These smooth lines are easily seen and can be identified against any background unless they are carefully concealed. The opposite is of course true in urban situations, where straight lines occur throughout the background, and should be matched during concealment.



The unmistakable shape of skylined equipment

1. AAP-6.

6. **Shadow.** Shadow can be divided into two types:
 - a. *Cast Shadow.* Cast shadow is the projected silhouette of an object against its background.
 - b. *Contained Shadow.* Contained shadows are the dark pools of shadow which are formed in areas that are permanently in the shade. Examples are inside a slit trench, under vehicles and inside open cupolas. These shadows show up darker than their surroundings and are easily detected.
7. **Shine.** Glass and shiny surfaces reflect and at times magnify light. All glass and shiny surfaces must be covered as a priority during even the shortest of vehicle halts.
8. **Movement.** Movement against a stationary background will always attract attention. It must be kept to a minimum. When movement is necessary, slow regular movement is usually less obvious than fast erratic movement. Movement also produces dust, tracks and heat, all of which can be detected.



Dust and Exhaust

9. **Colour.** Colour is important at close ranges but less important at long range. At very long ranges colours tend to merge into an even tone. In limited light the eye cannot discriminate colour and is only able to distinguish contrast.
10. **Pattern.** Pattern affects camouflage in two ways:
 - a. *Pattern of Equipment to its Background.* The pattern of the background against which military equipment is viewed changes constantly. The relationship of equipment to its background varies with the distance at which the object is viewed and the distance between the object and its background. All of these

factors are variable which makes it difficult for an object to have a pattern that will blend with all backgrounds.

- b. *Terrain Pattern and Military Activity.* The pattern produced by the siting of equipment and vehicles and made by tracks must conform to that of the natural terrain.
11. **Texture.** Texture is the structure of a surface. A rough surface will appear darker than a smooth surface even though they are both the same colour. The most important aspect of this factor is tracks. The passage of a vehicle will change the texture of the ground, even if the surface is not broken, causing track marks to be clearly visible, particularly from the air.



Poor track discipline is obvious from the air

12. **Electromagnetic Signatures.** The characteristic electromagnetic signatures of an object that make it most identifiable are in the Visible, Near Infra-Red, Far Infra-Red (Thermal), Radar and Radio bands. Minimizing energy emissions in these bands will therefore make it more difficult for the enemy to detect the presence of a target.

SECTION 3 - PRINCIPLES OF CAMOUFLAGE

13. The factors of detection are interrelated and when considered together allow objects to be recognised and identified. When planning countersurveillance measures the following principles apply:

- a. Careful siting of equipment.
- b. Camouflage discipline.
- c. Correct use of camouflage materials.

Careful Siting of Equipment

- 14. Careful selection of a position is essential in a countersurveillance plan. A good position will often provide good concealment with little need for assistance from artificial camouflage materials and less destruction of surrounding areas.
- 15. Initially, a future position or site will be selected from the detail provided on a map. A detailed ground reconnaissance is required to complete the terrain study before a position is selected. Care should be taken during the selection process to allow for natural routes into and out of the position.
- 16. Points to note during a site reconnaissance include:
 - a. *Buildings.* Built up areas give the opportunity to disguise military activity amongst local activity. There is an abundance of rubbish and loose material in an urban area, which could assist in concealment of military equipment.
 - b. *Woods.* Thermal imagers are capable of penetrating certain types of foliage. Care should be taken to ensure Thermal Camouflage Woodland (TCW) is used when in wooded areas. Particular attention has to be paid to covering up "hot spots" such as vehicle engines, exhausts and generators.
 - c. *Shadow.* Maximum use should be made of natural shadow to break up outline, remembering that it moves as the sun moves. Parking in shadow also means that the shade from the sun will reduce the solar loading so that vehicles will not become prominent thermal targets because of sunlight.
 - d. *Dead Ground.* Dead ground gives protection from ground surveillance and should be used to conceal movement. However, it does not provide protection from aerial surveillance.
 - e. *Ground Pattern.* There is a need to match the existing ground pattern by alignment with hedgerows and buildings and using existing tracks that conform to the local pattern.
 - f. *Isolated Cover.* Avoid using associated and obvious cover. These areas will be under constant surveillance by the enemy.
 - g. *Soft Surfaces.* Where possible, soft surfaces should be avoided as they clearly show track marks and are difficult to camouflage.

Camouflage Discipline

17. **General.** Successful camouflage requires constant attention to detail and frequently involves tedious and time consuming work. Camouflage discipline is essential and should be based on knowledge of the surveillance threat. One mistake can ruin the best camouflage plan. The most important aspects of camouflage discipline are:
 - a. Practice.
 - b. The use of drills and procedures.
 - c. Track and movement discipline.
 - d. Control of heat sources.
 - e. Personal camouflage.
 - f. Camouflage SOPs.
18. **Drills.** The chances of mistakes can be minimized if simple drills are followed to carry out routine tasks. Camouflage drills include:
 - a. *Halting.* Vehicles should never halt in the open. They should move off the road under cover of trees or the shadows of hedges or buildings. There may not be time to use nets, but reflective surfaces should always be covered.
 - b. *Harbouring.* The key to success in harbouring is reconnaissance. Harbour drills include:
 - (1) A track plan.
 - (2) Site selection for individual vehicles.
 - (3) Vehicles should not stop outside the harbour but should move straight to their position. This may require guides or signs.
 - (4) If the reconnaissance is not finished before the vehicles are due to arrive they have to be held in an area away from the harbour.
 - c. *Layout.* In many circumstances a standard layout of vehicles will assist in the speed of the reconnaissance and harbour occupation and thus in the speed of achieving good concealment. However, the layout should not be so rigid as to allow the enemy to identify the unit by its layout pattern.
 - d. *Visitors.* A procedure for receiving visitors and their vehicles is essential. A hide needs to be selected for visitors' vehicles and a net may have to be erected. Sentries/guides are to be briefed to ensure that visitors are quickly directed to put their vehicles under cover.

19. *Unit SOPs.* Unit SOPs will highlight other procedures in the harbour drills. Unit drills need to be flexible to allow the most important aspects of camouflage to be completed first.
20. ***Track and Movement Discipline.*** Track discipline is essential. A track plan should be prepared before a unit moves into an area and both vehicles and troops should adhere to the plan. Where new tracks have to be made they should fit into the existing pattern and appear logical. Movement must be kept to a minimum and be planned and coordinated. Maximum use should always be made of cover and dead ground.
21. ***Heat Sources.*** As far as possible heat sources should be shielded from likely surveillance sensors. Maximum use of dead ground for heat sources need to be used. Hot exhausts should point away from the enemy. All activities which produce heat have to be controlled and kept to a minimum. These include:
 - a. Vehicle engines.
 - b. Generators.
 - c. Cooking equipment.
 - d. Lighting.
22. ***Personal Camouflage.*** Personal camouflage includes:
 - a. Dressing correctly and wearing camouflage cream.
 - b. Remaining in the shadows and not resting in the sun.
 - c. Not lighting cigarettes in the open, by day or night.
 - d. Conforming to track plans.
 - e. Not looking up at overflying aircraft.
23. ***Camouflage SOPs.*** Good camouflage SOPs cover the occupation of operational positions, the maintenance of camouflage plans during occupation and a careful evacuation plan to ensure nothing of any value is left behind. Camouflage discipline has to be maintained during all of these phases. The enemy can gain a lot of information after a unit has left an area from the traces which are left there. Discipline needs to be maintained at all times.

Correct Use of Materials

24. ***General.*** Camouflage materials can be divided into those which are permanently incorporated into an equipment and those that are temporarily attached. Permanently incorporated materials such as paint schemes normally affect the colour and

surface texture of the equipment. The most common temporarily attached materials are camouflage nets and vegetation.

25. **Colour.** The basic colour of an equipment must not stand out in contrast to a background. The colour or reflectivity should extend into the infra-red band to assist in giving protection against infra-red photography and night viewing devices. The surface texture should be sufficiently rough to eliminate shine.
26. **Clothing.** Disruptive pattern camouflage clothing should be worn in all areas of operation. The particular type of camouflage clothing to be worn will be identified by the area of operation, ie disruptive colours for wooded areas and white for snow conditions. Issue disruptive pattern camouflage clothing for use in temperate climates has a near infra-red reflective capability.
27. **Disruptive Painting.** Disruptive painting is used to distort the visual appearance of an object. The disruptive painting should not contain any colour or shade that is greatly different from its background. Only issue camouflage paint should be used for camouflage purposes. The green paint on issue for use in a woodland environment is an infra-red reflectant, matt paint. The disruptive paint coverage should be approximately 2/3 green and 1/3 black. The painting of equipments is covered in detail in Materiel Regulations for the Army Volume 2, Pamphlet 4, Section 5 (Army Code 60503). In snow conditions a paint scheme of 2/3 white and 1/3 black should be used. In other words, the green should be overpainted with white. Two techniques of camouflage painting that can be employed separately or together are:
 - a. *Pattern Painting.* This technique makes the object appear as a number of unrecognisable shapes. This is achieved by using large bold patterns and contrasting colours over all surfaces.
 - b. *Shadow Distortion.* This technique aims to distort normally distinctive shadow areas on vehicles with black paint.



Disruptive paint pattern in snow

28. **Woodland Camouflage Nets.** Camouflage nets are used to break up the shape of a target and to help it blend with the background. A net is used in preference to a continuous sheet because the latter, however patterned, will always show up as a solid patch when viewed from a distance against a variegated background. Although a net may appear transparent when viewed from close range, if correctly erected and supported away from the equipment, it will give good camouflage when viewed from realistic enemy surveillance ranges.
- a. *Mark 5 Woodland Camouflage Net.* The Mark 5 woodland camouflage net has a 100 mm x 100 mm nylon mesh with polyurethane coated nylon garnish patches. The nets come in various sizes, and are lightweight. The net has approximately 66% garnish cover at its centre and approximately 60% garnish cover towards its edges. The patches are coloured green on one side and brown on the other. The net is reversible to enable it to be used with a combination of 2/3 green and 1/3 brown on one side or 2/3 brown and 1/3 green on the other side depending on the prevailing conditions. The Mark 5 net requires garnishing with local foliage to assist it to blend with the environment.
 - b. *Mark 7 Woodland Camouflage Net.* Mark 7 nets are issued as part of concealment sets for all high value equipments. The Mark 7 net has a 75mm x 75mm mesh made of a stronger, non absorbent nylon than the Mk 5 net. The Mk 7 net is reversible in the same way as the Mk 5 net and has improved colouring to help it blend with the environment. It has a higher percentage of garnish patch cover and should not need any natural foliage to be added. The net also has 'Dutch Lacing' loops along its sides to allow for easy joining to other nets.

Concealment Sets

29. **General.** Vehicles and equipment that have been designated high value battlefield assets are issued with concealment sets. Concealment sets reduce the time required to camouflage and cater to the requirement of particular equipments, eg guns traversing and firing under camouflage. These sets consist of thermal camouflage material and specially sized nets supported by poles or frameworks using spreaders to minimise unnatural peaks in the nets.
30. **Camouflage Support System (CASS).** CASS is based on 1.2 m long glass reinforced plastic (GRP) rods which join together to form either a ground or vehicle mounted support system. The rounded outline produced by CASS hoops should be disrupted by using CASS rods fitted with spreaders. Some sets still use the old, stronger but heavier, alloy poles.
31. **CASS Accessories.** Each CASS set contains the following accessories:
- a. Lightweight camouflage net spreaders (plastic and cruciform), for use on the ends of CASS rods.
 - b. Ground spikes for poles and nets.

- c. Mallet.
- d. Small bungees for joining the CASS hoops where they cross over, to provide the supporting structure with more rigidity.
- e. Carrying bags.
- f. TCW toggles and bungees.



Camouflage Support System (CASS)

- 32. ***Vehicle Mounted CASS.*** The CASS system can be attached to vehicles by using tubular brackets which are welded onto the vehicles when the concealment sets are issued. These tubes allow the system to be rapidly erected and removed by providing a firm base for the structure of GRP rods. They are particularly useful at night. Once the hoops of rods have been made over the vehicle the camouflage net can be easily drawn over them without snagging on the vehicle.
- 33. ***Ground Mounted CASS.*** The system contains ground spikes, which have tubes welded onto them, to allow easy erection of a shelter which is not attached to the vehicle or equipment being camouflaged. The spikes should be driven into the ground at a distance of approximately 2 m from the edge of the equipment, to ensure that when the hoops are bent over, they do not come too close to the equipment. The system is then used as for a vehicle mounted system.



Ground mounted CASS poles



Mark 7 net with CASS

34. **Crew Instruction Card.** Each concealment set is issued with a set of crew instructions on a laminated plastic card. These should always be consulted before training troops in the use of the concealment sets.
35. **Thermal Camouflage Woodland (TCW).** TCW is a thermal sheet that is fitted over the hot areas of a vehicle. The sheet greatly reduces the thermal radiated energy emitted from the vehicle. TCW will melt if placed directly onto very hot surfaces, eg exhausts. Therefore thermal isolating mats and cages are issued to avoid damage to the TCW by very hot surfaces. TCW is not to be used without a camouflage net. Without a camouflage net, TCW would be visible to a TI sensor as it would show up as a cold object compared to its surroundings. The camouflage net must be supported 0.5 m clear of the TCW to avoid the net being heated by the TCW and becoming detectable. TCW is issued with rubber toggles and bungees with which the sheets can be joined together and held in place on the vehicle. The TCW 'skirts' on MBTs can be rolled up and fixed to the hull. Damaged TCW can be repaired with masking tape.



TCW on Warrior

36. **Safety.** The GRP rods will split if bent through too tight a radius. Therefore the vehicle mounting method must only be used on those vehicles provided with an agreed modification kit. Care must also be exercised when inserting or extracting the rods from vehicle mounted brackets or ground spikes.
37. **Snow Concealment Sets.** Concealment sets with white thermal camouflage material - Thermal Camouflage Arctic (TCA), white nets and CASS are issued to units with an operational role in snow conditions.

Vegetation

38. The application of vegetation will greatly help in giving a natural look to camouflage. Its main disadvantage is that it wilts and requires replacing. Vegetation retains its correct reflectivity in the near infra-red band until after it wilts visibly to the eye. However, it is detectable using False Colour Imagery. Some types of foliage wilt quicker than others with various types lasting from a few hours to over a week. The following points should be remembered when cutting foliage for camouflage:
- a. Choose branches which have been growing in direct sunlight. These stay greener much longer than branches from the same tree grown in the shade. (The reverse may be true in the tropics, depending on local conditions.)
 - b. Cut foliage with leaves which feel tough to the fingers.
 - c. Place the foliage in the same state as when it was growing. The undersides of leaves give an unnatural appearance and also turn brown quickly in the sun.
 - d. Coniferous trees such as pine and spruce have the best lasting qualities.
 - e. Do not cut from only one area and avoid leaving scars on the extremities of woods.
39. The use of vegetation will also shield the vehicle from the heat of the sun and hence its thermal signature will not increase as the sun shines. Cut vegetation will only heat up at the same rate as the surrounding ground so a contrast will not be created. Exposed metal of vehicles heats up more rapidly than natural materials and soon contrasts with the natural background.

Other Materials

40. For camouflage to be completely effective, additional materials are required such as Cloth Camouflage Synthetic Olive Drab (CCSOD), poles, pegs, rope and string. Except for CASS and CDM these items are not issued specifically for camouflage purposes but are available from unit resources.

Camouflage Procedures

41. The following procedures should be followed when camouflaging equipment:
- a. Site carefully under or near natural cover.
 - b. Cover reflecting surfaces, eg windscreens, lights and mirrors. Cover contained shadows by lowering back canopies and placing hessian, CCSOD or brush-wood around the bottom of vehicles and equipment.
 - c. Select the appropriate side of the net to use and drape it over the equipment. Peg the net to the ground at least 2 m away from the equipment. Where applicable, the CASS and TCW are fitted prior to erecting the net.

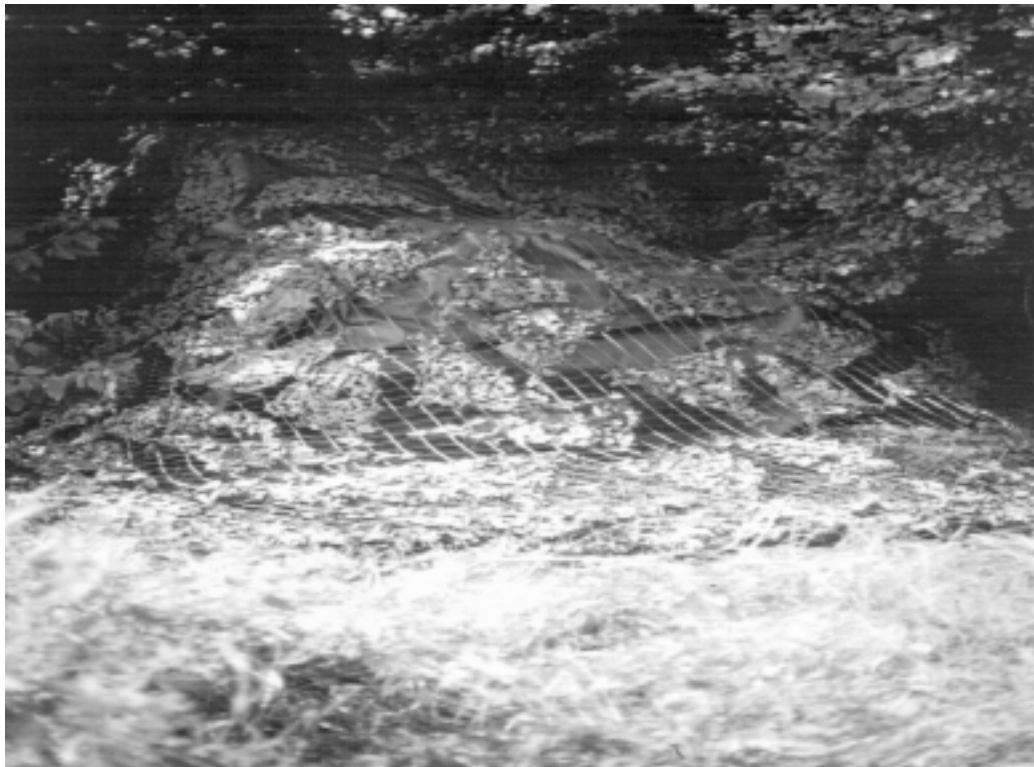
- d. Push the net out using poles and spreaders. This is especially important along straight edges and at corners. The net must be at least 0.5m away from the equipment so that shadows can form and the minimum of light is reflected from underneath.
- e. Add vegetation if required.



The Stages of Camouflage: Site the vehicle



The Stages of Camouflage: Cover shiny and reflecting surfaces



The Stages of Camouflage: Drape the net and peg 1-2m from vehicle

Temporary Halts

42. For temporary halts of only a few minutes, it may be acceptable to position under existing cover and only cover shine and shadow areas. For halts over 15 minutes, camouflage nets must be used, unless the local tactical situation dictates otherwise.

Camouflage in Urban Areas

43. **General.** Where possible in urban areas, equipment should be inside buildings or camouflaged to blend with the buildings and not vegetation. In these circumstances Urban Camouflage Material (UCM), tarpaulin, corrugated iron (CGI) and plastic sheeting are more suitable than a camouflage net. Shapes are more important than colour and should be straight and angular, not rounded. Wherever possible the existing shapes of the buildings should be extended to include the camouflaged equipment. In a farming community, maximum use of local materials such as haystacks, out-buildings and farm equipment will help camouflaged equipment blend in with the local environment. When siting equipment next to buildings, care should be taken so that the equipment does not look out of place or like a strange add-on feature. In urban areas it is easier and more effective to conceal a vehicle in a shed or garage than to attempt to make it look like a building. In all situations care has to be taken so that moving shadows do not betray vehicles pushed under overhead cover.
44. **UCM.** UCM is issued in rolls 3.5 m wide x 60 m long. Eyeletting kits are separate items and should be used when required; 2 kits are needed for each roll. UCM can be used in two ways. It can be used to completely cover a vehicle or equipment, or it can be hung from the eaves of roofs and dutch barns. When used as a vehicle

sheet, UCM should be tailored to the size of the equipment to be camouflaged. This sheet then becomes part of that equipment's dedicated camouflage material. Eye-lets should be put into the material at 1-2 m spacings, to enable the UCM to be tied or pegged down when in use.

45. **UCM as a Drape.** When hung from the eaves of roofs, the UCM should preferably be nailed in place then cut to size and secured firmly to the ground. If the material is not secured at the bottom it will move in the wind and this movement will attract unwanted attention. Military equipment can be easily and effectively concealed behind drapes of UCM.



UCM hung as a drape from the eaves of a roof

46. **Siting.** As with all camouflage, siting of urban positions is very important. If possible, equipment should be positioned on the north side of buildings to utilize existing cast shadows. Thought should be given to positioning on the downwind sides of buildings, to lessen the effect that wind has on UCM, both when deploying the material and when camouflage is complete. Once the equipment has been positioned and before work starts on camouflage, the position should be viewed from a distance of about 100 m. This is to ensure that the equipment is correctly aligned with existing buildings and that existing straight lines and angles have not inadvertently been disrupted. If the line of windows or doorways is disrupted care should be taken that it is disrupted by a straight line across the whole of the aperture, so as not to draw attention to the position.
47. **Use of Material.** Before covering the equipment with UCM every effort should be made to "square" the equipment off to achieve large regular shapes that will blend with the urban background. Lorries and Land Rovers pose a particular problem in this respect.



Use of locally available material to hide a Land Rover



Farm material used to disguise a 4 Ton Vehicle

- a. In the case of a Land Rover, if the bonnet is raised and a sheet of timber laid from the canopy to the raised bonnet an almost perfect rectangular outline can be achieved. For transit, the board or boards can be inserted between the canopy and the superstructure of the vehicle.
 - b. Large load carrying vehicles are slightly more difficult to camouflage, but a great deal can be achieved by good preparation before deployment. By lashing convoy flag-poles to wing mirror arms, anything which is draped over them will raise the apparent height of the cab to the same height as the canopy, to give a regular rectangular outline. Care must be taken during peacetime to avoid damaging the vehicle structure. Troops should be encouraged to experiment with urban camouflage materials to find the best method to camouflage vehicles in an urban area and any worthwhile short cuts disseminated as widely as possible.
48. **Safety.** If vehicle engines are run under UCM, then it is possible for a build-up of exhaust fumes to occur. Units should be aware of this potential problem and, if soldiers are required to work under UCM, eg manning radios or routine servicing, they must ensure that exhausts are adequately vented.

Cold Weather/Snow Camouflage

49. In snow conditions special (white) camouflage clothing, paint and nets can be used. However, these sorts of camouflage material are not normally issued for use in areas where it only snows occasionally. In these circumstances it is necessary to improvise to achieve a 2/3 white aspect for individuals, vehicles, equipment and nets. Winter camouflage can be improvised as follows:
- a. *Individuals.* Strips of white material or tape attached to combat suits and personal equipment.
 - b. *Vehicles and Equipment.* Removable white paint can be applied to the green areas of disruptive paint patterns. A German whitewash called KALK can be used when operating in snow, although while easy to apply, it can be difficult to remove from canopies and exhausts.
 - c. *Nets.* Strips and patches of white material can be made from old laundered bed sheets but the pattern of the applied patches has to resemble the broken snow cover when viewed from both the ground and the air.

CHAPTER 3

SPECIFIC ASPECTS OF COUNTERSURVEILLANCE

SECTION 1 - THE SOLDIER

1. **General.** Soldiers have to be trained in countersurveillance techniques to conceal themselves from both ground and air observation by day and by night.
2. **Ground Observation.** Soldiers need to be made aware that most armies possess highly trained observers equipped with advanced surveillance devices. They have to be made aware of the potential of such observers, preferably by demonstrations of the effectiveness of these equipments.
3. **Air Observation.** The most common mistakes made by soldiers when endeavouring to conceal themselves from air observation are:
 - a. Failure to visualize what the ground looks like from above.
 - b. Failure to hide spoil and conceal weapon pits, equipment and tracks.
 - c. Looking up at aircraft.
4. **Individual Camouflage and Concealment.** The aim of individual camouflage and concealment is to defeat enemy observation. Successful concealment means that the soldier can observe and operate against the enemy without being seen himself. Chapter 2 lists the 8 factors by which an object may be recognized and distinguished from the background against which it is sited. These factors also apply when considering personal camouflage. Particular attention should be paid however to the camouflaging of helmets, mess tins and personal spectacles or wristwatches. Exposed skin should be dulled or shaded whenever possible.

SECTION 2 - DEFENDED LOCALITIES

Countersurveillance Measures

5. **Preliminary Reconnaissance.** Movement and unnecessary tracks made during reconnaissance or siting of a position may indicate to the enemy points to watch. The final reconnaissance of each site should be made on foot.
6. **Planning.** Concealment of a position has to be planned and conducted systematically:
 - a. Post sentries to warn and protect the construction of the positions.
 - b. Avoid all unnecessary noise.

- c. Site positions to conform with the natural ground pattern.
 - d. Make a simple track plan following the same pattern, and ensure that it is concealed wherever possible. Even a lightly-used foot track can be detected on aerial imagery.
 - e. Enforce this as the only track plan from the start.
 - f. Hide defence stores until they are ready for use.
 - g. Mark out each fire trench. Work from within these marks.
 - h. Roll the turf and the weathered surface soil away from the trench on every side. Keep this free from dug-out spoil.
 - i. Layer the spoil evenly around the trench as it is dug out.
 - j. Roll back the turf and replace the old surface dirt over the freshly dug spoil and hide it.
 - k. Remove any surplus spoil into cover nearby. Hide it along hedgerows, at the foot of trees or among debris.
 - l. Where trampling is unavoidable, disguise it afterwards.
 - m. Where mechanical equipment is used, strict track discipline is to be enforced during the preparation of the position.
7. **Siting.** Good fire positions are essential. Site them for surprise and protection. A second choice that gives concealment is preferable to an obvious site that invites destruction. Site within the ground pattern. If possible avoid making parapets; ground level gives better protection and concealment. Fit the position into the existing pattern. Special care needs to be taken when siting surveillance devices (eg radar, OTIS) so that operators can carry out their task with minimum risk of disclosing either themselves or associated defensive positions.
8. **Overhead Cover and Protection.** A fire trench shows as an open dark shadow when viewed from above. Overhead cover can eliminate this feature, as well as giving some physical protection. It can be provided in 3 forms:
- a. Light frame lids merely to conceal. These offer no physical protection and are designed to be thrown off to engage the enemy.
 - b. Trench shelters to provide overhead protection (OHP) alongside the fire position within the same trench. These offer concealment and protection from the splinter effects of low air burst shelling. The shelter is made with its roof at ground level to aid concealment.

- c. Emplacement of overhead protection to provide protection from solid missiles and blast, and cover from beneath which a weapon can fire. This type of OHP protrudes above the ground level of the weapon it covers. It makes effective concealment more difficult and requires greater effort. Overhead protection should be splinter proof; however, the hard outline over the dark shadow is made worse by the light that outlines soldiers' heads. The desire to gain all round observation creates this risk.
9. **Weapons and Equipment.** These present 3 main concealment problems:
- a. How to keep weapons concealed so that they cannot be observed or associated with any particular arm or unit.
 - b. How to disguise the special characteristics of their firepower.
 - c. How to minimise the movement associated with replenishment, for example resupply of ammunition.
 - d. Maintaining the operational capability of the weapon underneath camouflage.
10. **Command features.** Distinctive weapons, clothing and equipment, eg binoculars and map cases, may indicate the commander in a unit or sub-unit. These features must be disguised in the field. This also applies to such equipment as radio sets and aerials.

SECTION 3 - ARMOUR

General

- 11. The size and shape of armoured vehicles make them difficult to conceal. For this reason, tanks and armoured vehicles will normally be dispersed in troop or well dispersed squadron hide positions where they can be hidden from ground and air observation. They will generally not concentrate for an attack before it is necessary to do so, nor move into defensive positions until the enemy threat develops.
- 12. The time and effort spent on the camouflage of armoured vehicles in hide positions will depend upon the expected duration of their stay and their next likely task. Unit commanders must ensure that all AFV commanders are given this information as soon as possible. The introduction of new surveillance sensors emphasizes the need to maintain countersurveillance measures both by day and by night.

Movement

- 13. Movement, or the evidence of past track movement, catches the eye immediately.
 - a. *Routes.*
 - (1) Tracked vehicles leave distinctive scars. Movement should be along existing roads or tracks, or on the edges of fields and woods where there are shadows.

- (2) Once tracks are made they are almost impossible to hide. Tracks on the edges of woods where armoured vehicles have turned or reversed are easily identified from the air. Wherever possible turns must be made under cover. Track scars have to be covered over.



Tracks at the edges of woods point towards the hide

- b. *Dust.* Dust denotes movement. It attracts the eye and could bring down fire. Low speeds will reduce dust.
- c. *Smoke.* Vehicle exhaust smoke will attract attention and every effort should be made to conceal it by moving behind cover. Drivers have to learn the appropriate driving techniques for their vehicles and in particular build up engine revs slowly and switch off when possible. Tank drivers are also taught to maintain a 'decoked' generator unit engine exhaust, to reduce exhaust smoke.
- d. *Noise.* Engine noises, voices and radio, the clatter of jerricans during replenishment and the sounds of crews and fitters working on vehicles, can all be heard at long distances. Good noise discipline and careful driving in the correct gear, keeping engine revolutions down, will reduce noise levels. Radio gains should be reduced and loudspeakers turned off. Auxiliary generators should be switched off or only used when essential, when close to the enemy. In a static hide position it should not normally be necessary to run the auxiliary generator.
- e. *Security.*

- (1) Care has to be taken to avoid disclosing AFV positions by unnecessary

movement of men or vehicles, especially during replenishment, maintenance or repair.

- (2) Tank commanders should plan a series of alternate fire positions. Moving to alternate fire positions, or jockeying, is a useful manoeuvre during a long range engagement of dispersed and static enemy. However, it is most unlikely to be used during a troop or squadron action against an enemy which is concentrated and on the move, because it takes too long to get back into a position to engage the enemy.
- f. *Routes.* Routes need to be carefully chosen to screen movement from enemy observers or surveillance devices. This is best done by making maximum use of dead ground. When in contact smoke can be used to screen movement but has the disadvantage of attracting the enemy's attention.

Shine

14. Many objects reflect light:

- a. Matt paint may shine where it has been polished by men climbing over vehicles. Particular attention should be paid to gun barrels; different types of gun each present their own problems.
- b. AFV tracks shine. The tracks of AFVs need to be hidden when in static positions.
- c. Fires, smoking and lights show for long distances at night.
- d. Optical instruments may reflect the sun and should be shaded if possible.
- e. Episcopes and periscopes need to be masked and all hatches/doors closed before interior lights are switched on at night. Blackout switches should be used where fitted.

Shadow

- 15. The concealment of vehicles can be assisted by positioning them where shadow falls over them or where their shadow falls into a broken background. An AFV contains characteristic shadows particularly in the area of the suspension and between its turret and hull. This contained shadow can be disguised by pattern painting, but the crew need to further camouflage it with foliage or a net in defensive positions.

Shape

16. The following aspects of shape should be borne in mind:

- a. Foliage attached to canopies, skirting plates or turrets will break up their distinctive shapes.

- b. Camouflage must look natural and be correct for the surroundings. It must be kept fresh.
- c. In farms or built-up areas foliage is inappropriate. Baulks of timber, hay or farm materials should be used.
- d. Vehicles should be hidden in buildings when this is possible or in dead ground until they adopt fire positions.
- e. Circular openings, such as cupolas, are especially distinctive from the air and must be broken up or covered.

Heat

- 17. The issued TCW should be used to conceal the prominent thermal signatures of AFVS. In addition, AFVs should be positioned wherever possible so that prominent hot areas are screened from enemy view by aspect, terrain or buildings.

Tactical Considerations

- 18. Camouflage is the responsibility of vehicle commanders at all levels and a high standard of concealment has to be maintained by discipline, training and personal example. Troops should camouflage their vehicles as a matter of course when on tactical training and standards should not be allowed to deteriorate when crews are tired.
- 19. Careless use of camouflage nets or natural camouflage may interfere with the fighting efficiency of the vehicle. Periscopes and sighting gear must not be covered; the gun must be able to traverse freely and aials must be clear. Camouflage is a fire hazard when it is in contact with the engine or auxiliary generator exhaust systems.
- 20. An AFV commander has many factors to consider when choosing a fire position. He will always make the best use of available cover and will use other measures as circumstance permits:
 - a. Vehicles should move slowly to avoid dust and exhaust smoke when approaching their fire positions.
 - b. The position of the vehicle should be selected in relation to the background and enemy viewpoint. On no account must the whole vehicle be silhouetted against the skyline. Commanders must ensure that the minimum is exposed to the enemy during observation and firing.
 - c. The vehicle commander should plan the best route to his next fire position, whenever possible choosing a route which will expose him to enemy fire for the least possible time.
 - d. Defensive positions should be reconnoitred before occupation and a proper track plan drawn up before the arrival of vehicles. Metalled road surfaces

(which do not readily show track marks) and tracks should be used wherever possible. Approaches covered by trees should be used where suitable tracks do not exist.

- e. Buildings may sometimes be used as fire positions provided that there is sufficient space to traverse the gun through the required arcs. However, there is a danger that enemy fire may collapse a building on top of an AFV, and so trap it.
21. When it is necessary to concentrate a complete group in one location, special security arrangements have to be made to control late arrivals, echelon vehicles, fitters and visitors. An RV equipped with radio should be established some way from the concentration area, where those joining the grouping can wait under cover until it is safe to move forward. Unnecessary noise, smoke and lights must be avoided in the concentration area. An alternate RV and concentration area must be designated in case it becomes necessary to move at short notice.

Summary

22. Good concealment is achieved by proper planning and firm discipline at all levels. Planning should be carried out in 2 stages:
- a. AFVs are to be prepared and equipped for concealment before operations begin. This preparation will include camouflage painting, maintenance of camouflage nets and the provision of poles and other materials for each vehicle.
 - b. Clear directives need to be given to AFV crews as to how long they can expect to remain in a position. They can then assess the risk of being discovered and take appropriate steps to conceal their vehicles. Thus, time and effort will not be wasted in taking elaborate camouflage precautions in a position that is only to be occupied for a short time.

SECTION 4 - ARTILLERY

General

23. Artillery can only fulfil its task of destroying or neutralizing the enemy when it is not moving. It has to remain in action for as long as possible before moving to a new position. Artillery should therefore have high standards of camouflage, concealment and movement, and understand all aspects of countersurveillance.
24. The decision on how far countersurveillance methods will interfere with the provision of fire support will be a command decision, based on the enemy surveillance capability, the amount and the effectiveness of counter battery fire, and the air situation. Artillery is particularly vulnerable to the specialized surveillance systems designed to locate guns, mortars, rockets and radars.

Flash Spotting Threat

25. A flash spotting troop can locate guns and rockets, and can adjust counter battery fire on to the hostile battery positions. It relies on good visibility to achieve results using optical instruments but can use modern sensors to work through poor visibility. However, woods, dead ground, fog, smoke, and heavy rain or snow will reduce their effectiveness. The methods of observation and the likely accuracy to be achieved in average conditions are:
- a. Direct muzzle or booster flash - better than 30 m.
 - b. Direct smoke and dust - better than 50 m.
 - c. Indirect flash and sky reflection - 100-400 m depending on range and height of intermediate crest.
 - d. Indirect smoke and dust, and booster trails - 100-400 m depending on wind conditions, range and height of intermediate crest.
26. Flashless propellants have reduced the effectiveness of flash spotting, but all propellants make some flash and the occasional charge makes a very significant flash. The development of infra-red detection equipment could increase the effectiveness of flash spotting. In good visibility direct smoke and dust is visible for a considerable height above the battery.
27. Batteries should select positions which have sufficient cover to prevent the observation of direct flash, smoke and dust. It is generally true that the lower charges will produce less flash and smoke than the high charges. Therefore, when the surveillance threat overrides the normal requirements for accuracy, the gun position officer should select the minimum charge necessary to engage the target.

Sound Ranging Threat

28. Sound ranging troops can locate all calibres of guns and mortars to an accuracy of better than 100m and can adjust guns on to hostile batteries by sound adjustment. It is possible for sound ranging to locate any battery which fires, within locating range, to an accuracy dependent on the meteorological conditions and the range. Again the threat may be reduced by the use of the minimum charge.
29. Sound ranging can be “swamped” during periods of intense firing. The beginning and ending of such firings, however, and any brief lulls may offer the opportunity for occasional locations.

Radar Threat

30. Weapon locating radars are a threat to artillery which is firing in the high angle, or in the upper elevations of low angle. The threat can be minimized by the use of higher

charges and low trajectories, but this increases the threat of location by sound ranging and flash spotting,

Gun Lines

31. To achieve effective concealment of battery positions the following points should be noted:
 - a. *Variety of Layout.* Stereotyped layouts of battery positions and regular intervals between guns should be avoided. Dispersed positions can reduce location accuracy and increase protection against counter-battery fire.



The problem posed by salvage and packing on a gun position

- b. *Ammunition and Salvage.* The very large amounts of ammunition and salvage on a position are a major problem in concealing a field artillery position. Only a sufficiency of ammunition should be with the gun and if possible it should be dug in and camouflaged. All used packaging and spent cartridge cases should be covered and regularly removed from around the guns. Where possible ULCs should be held under good natural cover such as woods or barns, and the ammunition carried forward to the guns. In a position with poor cover, the salvage has to be removed completely from the position. Debris from the guns, such as cartridge bungs, will show up on aerial imagery, particularly in snow.
- c. *Cables.* Cables on the position need to be concealed by choosing a route offering natural cover, or by digging them in.
- d. *Blast Marks.* A blast mark appears from the air as a regular, fan shaped patch. On some types of ground such as heather, ploughed fields, stubble, tracks, roads, rubble, sand, rock and heavily shelled areas, blast marks either develop

slowly or do not show at all. On others, steps should be taken to break up the regular outline of the marks by such expedients as scattering lime, rubbish or ashes, or by placing brushwood mats or expanded metal sheets in front of the guns, and behind rockets.

32. The best defence against counter-battery fire is regular movement.

Air Defence Artillery

33. Air defence artillery positions are liable to be located by the same methods as mentioned above. The concealment of air defence artillery is, however, complicated by the following factors:

- a. The need to maintain continuous radar surveillance and control communications. The effectiveness of the air defence system is seriously degraded if electronic silence is imposed.
- b. The high state of readiness which is required by air defence weapons to engage high speed aircraft. Overhead camouflage nets have to be removed when the weapon is brought to a high state of readiness.
- c. The coverage requirements for both weapons and radars in the air defence role mean that the equipment may have to be deployed in exposed areas, with little natural cover.
- d. The high slew rate of some of the equipments limits the use of nets.
- e. The efflux from the booster motors creates a fire hazard to camouflage materials.
- f. Radars have additional technical problems which are:
 - (1) The attenuation of the signal by net camouflage materials.
 - (2) The power reflection from camouflage nets may damage the equipment.

34. Generally air defence has to rely for concealment on:

- a. Selecting a position which gives good natural camouflage background. Skylining should be avoided wherever possible.
- b. The use of purpose designed camouflage sets, backed up by local garnishing.
- c. The proper concealment of all other equipment on the position.
- d. The concealment of cables.

35. The large generators necessary on some air defence sites pose the additional problems of infra-red and audio detection. These can be reduced by hiding generators in barns or other suitable buildings but, if none are available, it may be necessary to dig in generators.

Locating Artillery

36. **General.** Survey processes involve the use of special markers which are visible at considerable distances. They are frequently sited on prominent features. Surveyors have to avoid giving away more information than is essential in carrying forward the survey. They should therefore use the least obvious method of indicating stations compatible with the process in use. Lights and lamps should only be used when absolutely necessary. Electronic distance measuring equipment should be switched on for the minimum time, and codes and correct procedure should be used on insecure voice circuits.
37. **Sound Ranging.** When cable is being used for communications, it should follow natural lines such as tracks, hedges and woods. Cable should be concealed from where it leaves the main cable laying route to the command post position, and should never run directly through the command post area. When radio link is being used, care should be taken to reduce the EW threat by correct siting on reverse slopes. Microphone positions should be concealed in natural cover.
38. **Weapon Locating Radars.** Weapon locating radars are best sited behind a low crest to screen them from ELINT sensors. The aerial should, where possible, have a good neutral background, and the main equipment and running gear should be camouflaged in the usual way. It is normally necessary to leave aerials free of camouflage.
39. **Meteorological Troops.** Balloons should be filled under cover and brought out into the open for only the minimum time before launch. The radar aerial should be camouflaged until shortly before launch.

Remotely Piloted Vehicles (RPV)

40. RPV positions should be sited under cover in dead ground with the Ground Data Terminal (GDT) sited behind a low crest, where it can maintain contact with RPVs while obtaining some protection from ELINT sensors. Launchers should deploy to the launch site as late as possible before launch and return to the hide immediately afterwards. Recovery vehicles should take similar precautions. The cables linking the GDT with the Control Station should be concealed. If possible the recovery position should be in dead ground and far enough away from the hide to maintain the integrity of the hide.

Command and Control

41. Effective surveillance of artillery positions can be reduced by the method of employment:

- a. *Control of Fire.* In certain tactical situations it will be necessary to control the fire of batteries. Part or all of the artillery may remain silent or 'masked' until it can be used in mass against a worthwhile target. Fire can also be controlled so that all guns in a regiment fire simultaneously, in order to "swamp" locating devices.
- b. *Pistol Guns/Sections.* Before a large fire plan it is desirable that pistol guns or sections carry out the adjustment of targets in order that battle positions are not given away. Pistol guns may have several positions.
- c. *Shoot and Scoot.* Weapons which are easily located, such as rockets and mortars, may have to adopt a shoot and scoot method of employment, in order to reduce the chance of effective counter battery fire. One firing position should not be used too often or too regularly.

SECTION 5 - ENGINEERS

Introduction

42. Engineer activity is relatively easy to predict when compared with other surveillance targets. This is because of the constraints on engineer work imposed by ground, which limits the areas where it can take place, and by timing, which dictates that it should usually precede other arms' moves. Because of these constraints, surveillance sensors can often be tasked to search for specific types of engineer activity in relatively small areas. The intelligence provided from such surveillance will contribute substantially to the enemy's knowledge of our overall tactical plan. This Section covers the main combat engineer operations in relation to the surveillance threat and indicates possible countermeasures.

Minelaying

43. Minelaying is likely to be a major activity during any conflict, particularly during the preparatory stages. The aims of enemy surveillance will be to determine the exact location and extent of minefields as they are laid. Minelaying activity has certain characteristics that enemy surveillance sensors will be trying to detect. These are:
 - a. *Movement.* During the period of laying the minefield, many vehicles and equipments will be involved, not only laying mines but delivering stores. The movement of these vehicles is likely to follow characteristic patterns, which can be detected not only by tracks, but also by the heat signature of the vehicles involved.
 - b. *Patterns.* Once laid, a minefield will tend to have a recognizable pattern. Characteristic furrows will be left by the minelayers.
 - c. *Concentration of Vehicles.* Once the minefields have been laid, the subsequent movement of vehicles through safe lanes may lead to concentration of these vehicles. It will also lead to the enemy knowing where these safe lanes are, unless these locations are disguised.



Furrows left by minelayers

44. Countermeasures should be based on the following:
- a. *Movement.* During the laying period, the number of vehicles involved must be kept to a strict minimum. All non-essential vehicles should be kept to the rear.
 - b. *Patterns.* Where standard minefield patterns are necessary, strict attention must be paid to the concealment of the mine rows themselves. Simple deception techniques can be employed to disguise their exact location, such as random tracks and furrows being dug in the area prior to the commencement of laying. The use of phoney minefields should not be ignored. Mine rows can often best be concealed by laying them along the edges of fields or in the middle of existing tractor routes.
 - c. *Concentration of Vehicles.* Strict traffic discipline has to be imposed. Concealed waiting areas must be prepared and movement between these areas must be strictly controlled.
 - d. *Speed.* As much advance planning and preparation as possible should be carried out well clear of the area selected for the minefield, to enable the time on site to be minimised.

Obstacle Crossing Operations

45. The enemy will make vigorous attempts to locate obstacle crossings. Such information will be of great importance to the enemy since, not only will it be a guide to the future tactical operations envisaged, but it may also provide targets for artillery strikes.

Deception measures should always be considered during the planning of obstacle crossing operations.

46. Enemy reconnaissance will be looking for obvious signs, such as the existence of good approach and exit routes to and from the obstacle. Normally such sites should be avoided; however, this may not always be possible since other sites may require a disproportionate amount of work on approaches to make them viable. Other concealment problems are:
 - a. *Equipment.* Depending on the nature of the obstacles and the nature of the equipment available, a considerable amount of equipment may need to be concealed in the vicinity of the chosen site. Every attempt should be made to disguise the location of the chosen crossing site until operations actually commence. This may mean that equipment has to be concealed at a considerable distance from the obstacle. Any reconnaissance of the selected site must be carefully planned to avoid attracting the enemy's attention.
 - b. *Concentration of Vehicles.* Once traffic has started to cross the obstacle, every attempt must be made to prevent an apparent concentration of vehicles at the obstacle. The maximum use must be made of good traffic discipline, concealed waiting areas and camouflage procedures. All unnecessary engineer vehicles should be removed from the area of the crossing site as quickly as possible when they are no longer required. Where possible, and where sufficient troops and equipment are available, a number of crossing sites should be used to avoid unnecessary concentration. Simple deception techniques can also be practised.

Demolitions

47. Demolitions, mainly bridge demolitions and route cratering, will form an integral part of any engineer obstacle plan. Enemy surveillance will give priority to detecting preliminary demolitions so that reserved routes may be predicted and subsequently identified.
48. Movement by engineer reconnaissance and working parties between chosen obstacle sites should be kept to a minimum. All working party vehicles should be kept well clear of work sites. Vehicles, stores and equipment should be kept well camouflaged at all times.

Field Defences

49. Engineer activity in assisting with field defences will normally be a regular feature of tactical plans. Engineers may be required to assist in preparing field defences in both battle positions and hides, particularly for headquarters. Earthmoving by mechanized equipment and explosives will be a main characteristic of these tasks.
50. Earthworks are vulnerable to detection by most surveillance sensors including normal visual reconnaissance. Strict attention should be paid to track discipline for the

movement of engineer plant and all unnecessary movement between work sites should be avoided. Natural vegetation should be used as quickly as possible to cover exposed earthworks. Where dummy field defences are dug as part of a deception measure, similar care should be taken in the concealment of any earthworks.

Support to Air Forces

51. Engineers are required to give substantial support to air forces in the field. Engineer work will normally consist of the preparation of short runways and VSTOL pads and the construction of hides. Although suitable access routes can be made and surfaced by engineers, these routes are difficult to camouflage, so existing routes, hard-standings etc should be used wherever possible. Special camouflage set are normally produced for the camouflage of aircraft in hide areas. The requirement for engineer support will be a continuous one, since the VSTOL detachments could frequently have to move to new sites.



VSTOL Aircraft Hide

Summary

52. Great care must be taken by engineers if early detection by the enemy of their work is not to prejudice the security of future tactical plans. Strict traffic discipline, good concealment techniques and the use of simple deception will contribute substantially to the success of these plans. Speed in completion of engineer work will be more important than ever before. This is true in respect of the ability both to react quickly to tactical requirements and to complete the task rapidly. A reduction in engineer working times reduces the amount of time available to the enemy for surveillance and target acquisition.

SECTION 6 - COMMUNICATIONS

General

53. Every level of command relies on communications. No matter what the size of the unit, the controlling organization can usually be identified by electromagnetic radiations from the location concerned and by the presence of cables, antennae, and generators associated with such a location. Complex communications equipment is a good indicator of command and control facilities, eg Formation HQs.
54. Direction finding equipment and other Electronic Warfare Support Measures (ESM) will locate communications equipments when they are transmitting but may not be able to pinpoint them with sufficient accuracy for target acquisition. The enemy, knowing the general area where a command element is situated, may attempt to discover its precise location by the use of patrols and/or aerial observation. The purpose of this section is to consider the principles involved in minimizing the chances of our electromagnetic radiations being intercepted and in concealing communications equipment from direct observation.

Electronic Security

55. The enemy derives intelligence from information gained by his ESM. First, by the interception of actual information transmitted over radio links and even in some circumstances over cables. Secondly, by locating transmitters and painstakingly reconstructing the organization of nets and communications links.
56. The most obvious way of denying information to the enemy is to adopt the EMCON procedure of electronic silence. When radio silence is broken the use of codes will deny information to the enemy. The most effective method is to use electronic encryption which disguises not only the message content but also any idiosyncrasies of the operator, such as accent, which might otherwise permit the enemy to identify a particular unit with a particular radio transmitter. On those nets for which electronic security equipment has been provided no transmission should be made in plain language, even when it is solely concerned with the engineering and setting up of the link.
57. On nets and links without electronic encryption, every care should be taken to prevent the adoption of non-standard voice and operating procedures which will make the net easily identifiable. Codes have to be correctly used on unprotected nets, to protect information of anything but the shortest term value.
58. Even when the measures discussed in the two preceding paragraphs are in force, there exists a danger that the enemy may be alerted by a change in the pattern of transmissions (traffic flow analysis). It is therefore important to try to maintain a constant pattern in message traffic and, during the build up to an important operation when traffic levels tend to rise rapidly, thought should be given to diverting routine messages to non-electronic means of clearance thereby absorbing the increased operational traffic without giving rise to an apparent overall increase. The use of

alternate means and minimising the use of radios is very effective in denying information to the enemy.

59. The enemy's DF threat is more difficult to defeat. However, there are actions which can be taken to reduce its menace over and above the obvious one of complete electronic silence which should be adopted whenever adequate alternate means of communication exist. Adherence to as many as possible of the following rules will create the maximum difficulties for the enemy's DF and intercept organization:
 - a. Adjust transmitters to the minimum power necessary for effective communication.
 - b. Use directional antennae and site them so that they enjoy the maximum terrain screening from the enemy. (This is a measure particularly applicable to vulnerable forward units in respect of their rearward communications).
 - c. Use short transmissions and keep them to a minimum.
60. If the enemy resorts to jamming, try to work through it. This may confuse the enemy into believing his jamming is inadequate. By immediately changing frequency one tells the enemy his jamming is successful. Only open up an alternate link as a last resort, as this will disclose more of our organization and resources. All units need to have SOPs and practised drills for actions to be taken in the event of jamming.

Concealment

61. Before examining the problem further it must be emphasized that concealment does not automatically result in a reduced communications capability. An antenna can be concealed from the human eye by being placed in the middle of a forest, but its communicating value may be considerably reduced. The same antenna can be sited at the edge of a forest and still be well concealed and at the same time provide good communications.
62. To achieve communication, if an antenna has to be sited above a tree line or on exposed high ground, it should be raised only so far as is necessary to achieve and maintain the appropriate communications.
63. The siting of HQs at all levels depends on a variety of circumstances. Although modern ground communications are mainly provided by VHF radio which requires line of sight for best performance, predictable high points need to be avoided. Often the less obvious and more easily concealed location on the side of a hill will provide equally good forward and rearward communications. Consideration should be given to siting radios so that communications run down valleys instead of over hills; this can be very successful at limiting enemy DF effectiveness.
64. When siting HQs or communications complexes, care has to be taken to avoid obvious choices of location such as proximity to conspicuous tracks or roads over high features, or the largest building in a village. It is to be assumed that the enemy will

automatically examine both map and ground for such obvious sites. Careful consideration will invariably produce acceptable alternatives.

65. The deployment and identification of the different types of signal units and equipment can be a valuable indication to the enemy of our dispositions and command locations. The siting of communications facilities will often dictate the siting criteria of headquarters and units of other arms.
66. Message centres are vehicle mounted and should not be separated from the headquarters they serve. In some cases it will be possible to remote radio and radio relay vehicles (and their antennas) to better communications sites some distance from the headquarters. This will often help to conceal the exact location of the headquarters although care must be taken to conceal any cables that link the communications vehicles to the headquarters.

Cable Systems

67. Signal cables, surface laid or buried, are easy to identify from aerial imagery when they run contrary to the normal ground pattern. They should be buried wherever possible to minimise the risk of damage by EMP. Concealment around points of origin has to be achieved by following existing boundaries and track patterns. The concealment of empty dispenser packs and cable drums is equally important.

Antenna

68. The following points are to be considered:
 - a. Masts and their guy ropes have to be within the camouflage pattern of the associated communications vehicle. If this is not the case, the vehicle, whose presence might have been ignored as being of little significance, will be more easily identified.
 - b. Guy ropes, antenna feeders and masts stand out against dissimilar backgrounds. They should be sited to blend with the surrounding area. For instance:
 - (1) Amongst trees.
 - (2) Against the vertical lines of a building.
 - (3) At a hedge or road junction where the stronger lines of the ground pattern will help to absorb those of the mast. To site masts in an open field is to invite attention.
 - c. In most cases, even with omni-directional antennae, careful siting can provide both concealment and good radio communications. In some cases sites which provide good concealment may have to be accepted in preference to positions giving better radio reception.

Summary

69. In considering the concealment of communications facilities, it is vital to think of both the concealment of electromagnetic radiations and physical concealment from direct observation by sight and sound.
70. Neither of these aspects can be considered in isolation and both must be taken into account in the overall countersurveillance plan.

SECTION 7 - HELICOPTERS

Introduction

71. **General.** It will be exceptional for landing sites to be under enemy ground observation and countersurveillance measures will, therefore, be primarily directed against detection from the air. Although concealment from infiltrators must be borne in mind, this will usually be a secondary consideration. The detection, by an enemy, of helicopters on the ground may well lead to the discovery of an otherwise well concealed unit or formation HQ. All arms are likely, therefore, to be affected by countersurveillance measures taken in respect of helicopters. There are a number of countersurveillance problems which are largely peculiar to helicopters and these are outlined below.
72. **Shine.** The construction of aircraft means inevitably that they give rise to shine, particularly from perspex and smooth surfaces. All helicopters carry their own lightweight covers to cover the main perspex areas.
73. **Shape.** Helicopters have a very distinctive shape; notably the rotor blades. They require a cleared area in which to land and thus when coming to rest will be exposed, from the air, against a relatively unbroken immediate background. The effects of this can be reduced by selection of an area in which the immediate background forms part of an overall broken pattern and the use of areas of shadow. Blade folding or the use of concealment devices may serve, in some degree, to reduce the distinctive shape. However, unless the background can be changed, the danger remains that the aircraft will still stand out as a camouflaged aircraft. The most practical way to overcome this problem of the local background is to move the aircraft.



Helicopter Camouflage

74. **Movement.** Various means of minimizing the problems of ground movement are under consideration but the ideal solution is still likely to be to select a site which has good, firm access to suitably concealed locations.
75. **Landing Points.** Although the actual landing point will almost invariably be out of sight of enemy ground observation, the entire approach flight path will not necessarily be free from observation, particularly by radar. Unless, therefore, special measures are taken, air activity may well compromise an otherwise well concealed locality. Army aviation has a particular technique known as "concealed approach and take off" (CATO) for minimizing the chances of the site being compromised by aerial activity. In its simplest terms CATO involves the selection of a let down point, 1000-2000m away from the final destination, out of enemy observation, the final approach being made at low level behind ground or other cover. The same procedure is adopted for take-off. Helicopters should never land next to headquarters and when tasked to land at a headquarters LS, the time spent there must be kept to an absolute minimum, ideally 1-2 minutes.
76. **Fragility.** The fragility of controls and control surfaces make it difficult to use conventional camouflage methods without risking damage to the aircraft and for this reason camouflage should only be undertaken by aviation personnel; even then it tends to take longer than for more orthodox vehicles. Rotor tips, tail rotors, etc are all very susceptible to damage and this limits the use which can be made of natural or artificial cover, and makes movement in restricted areas more difficult.
77. **Response Time.** If army aviation is to be used to maximum effect, response time must be reduced to the minimum. The more comprehensive the countersurveillance measures, the greater the response time is likely to be. Inevitably, a compromise must be reached depending upon the tactical situation. For example, armed helicopters on standby will require the removal of some or all of their camouflage, depending upon their readiness state.
78. **Servicing.** Aircraft require to be serviced. This necessitates activity around the aircraft and may involve the movement of considerable quantities of fuel. This aspect complicates the design of concealment equipment and emphasizes the need, whenever possible, to get the aircraft under cover. Under intensive flying conditions much of the servicing will have to be undertaken at night with the consequent need for light proof cover over the aircraft. It is policy to fly the aircraft back to rear areas for work to be undertaken in the echelons, wherever possible.
79. **Infra-Red Radiation.** All internal combustion engines are difficult to conceal from infra-red sensors. This is particularly so for aircraft engines, which operate at very high temperatures. These prominent heat sources have to be concealed when the aircraft are on the ground.

General Concealment Measures

80. The normal principles of dispersion, avoidance of regular patterns in layout, use of shadow and artificial or natural cover, and choice of correct background, apply to

aircraft in the same way that they do to any other vehicles. The first essential is therefore the selection of a suitable landing site which has an overall broken background, has room for dispersion and contains suitable cover into which aircraft can be moved, ideally over smooth and firm surfaces. Strict CATO procedures are the next essential in order to prevent the site being compromised by aerial activity.

81. Once an aircraft has landed the sequence, in order of priority, is:
 - a. Take immediate action to reduce shine, by the use of covers.
 - b. Move the aircraft, where possible, under cover, eg a barn or overhanging growth, or into a more suitable background, eg into shadow, alongside features such as hedgerows or lines of natural contrast such as the junction of two different types of crop.
 - c. Cover the rotors.
 - d. Conceal the remainder of the aircraft.
82. Normal concealment measures must be carried out to ensure that the other activities associated with aircraft, eg servicing, movement of bowsers, briefing of aircrew, siting of CPs, etc, do not draw attention to the location of the aircraft.

SECTION 8 - VEHICLE AND ROAD MOVEMENT

The Threat

83. Two aspects of countersurveillance need to be examined when considering vehicle and road movement, those of movement and stationary activity. The improved surveillance techniques available to an enemy threat to expose vehicles and road movement throughout the theatre of operations to high definition photography, radar and heat sensors. No area can be considered safe from surveillance and a high standard of concealment is required throughout the operational area, including movement in base areas. Movement will be difficult to conceal, and deliberate deception will have to be practised in order to mislead the enemy with regard to detecting locations, dumps and other operational movement.

Surveillance Characteristics of Vehicles

84. A vehicle is characterized by its relatively large angular shape, smooth surfaces, heat emission and requirement to use the road system whenever practicable. Off road and on frost or snow, it leaves characteristic tracks. Collectively, both in locations and on the move, vehicles tend to form regular and unnatural patterns which can draw attention to their presence. Vehicle crews may draw attention to vehicles if insufficient attention is paid to personal concealment.
85. At night both white and infra-red light from vehicles can expose routes and unit locations. Noise should also be considered where vehicles are employed in forward

areas. This includes noise from the engine, movement of the load and associated activities such as loading and unloading.

Preparation of Vehicles

86. All vehicles have to be prepared for concealment and a full set of concealment equipment should be carried at all times. The following additional points should also be noted:
 - a. Lights, including stop lights, indicators and cab lights, are to be dimmed and masked to prevent observation or detection by enemy surveillance sources.
 - b. Exhaust systems should be screened to reduce their heat emission signature.
 - c. Unit signs and other markings should be removed.

Concealment of Individual Vehicles

87. All stationary vehicles should be concealed. At short halts the individual vehicles should, whenever possible, be parked under cover or in deep shadow clear of the road or track surface. For longer periods, the vehicles should be camouflaged. Care should be taken when the background is selected. This will normally be natural (woods) or artificial with regular lines (buildings), and the vehicle's camouflage has to conform with this background. The driver should keep under cover, periodically checking the camouflage for wind damage and shadow movement, without making unnecessary tracks himself.
88. Vehicles under trees should have reflective surfaces covered, and nets draped. Vehicle nets should also be draped at night whenever practicable. Camouflage should always be checked at first light for overnight "damage". In desert areas and snow where it is not possible to conceal vehicles under natural cover, their size and nature should be hidden by the use of nets. Camouflage has to be given priority over all other tasks, except protection, when vehicles arrive in a location. Drivers should be given assistance by other personnel or should work in pairs to pull nets over their vehicles.
89. It is not possible to conceal a moving vehicle. Routes should be carefully selected and varied. Regular journeys at set times should be avoided. At night speed must conform with the lighting available.

Concealment of Groups of Vehicles

90. Where two or more vehicles are parked in the same area, the overall pattern of all vehicles must conform to the general background. Regular spacing and uniform attitude must always be avoided. Columns at halts are particularly vulnerable to detection for this reason. Areas for halts need to be carefully selected.

91. The movement of groups of vehicles is extremely difficult to conceal. In addition to the techniques for the movement of individual vehicles, when route conditions permit, regular spacing should be avoided to make it difficult for an enemy to determine the number of vehicles travelling together. Ideally movement should be by groups of up to six vehicles. Air sentries need to be provided by vehicle crews, whenever possible. The fullest use should still be made of darkness, fog and rain to cover vehicle movement; although modern surveillance techniques sometimes enable an enemy to detect movement even under these conditions.

Materials Handling Equipment (MHE)

92. MHE establish a regular track pattern as they manoeuvre to load and unload vehicles. Whenever possible they should be used on hard surfaces or in areas under good overhead cover.

SECTION 9 - STORES AND INSTALLATIONS

Stores

93. Although rear operations may be beyond the range of some battlefield sensors, location of stores depots will still be an enemy priority. However, in large stores areas there will be very little labour available to carry out camouflage work but there are a number of factors which can alleviate this shortcoming. Planning, careful selection and the layout of the area are the keys to concealing this type of target. The relative importance of different types of stores has to be assessed and the most important afforded the best protection. Built up areas and woods give the best concealment.
94. Where buildings are used for concealing stores, care must be taken not to disturb the normal pattern of civilian activity associated with them. It is no good dumping the normal contents of buildings out in the open so that their place under cover can be taken by military stores. This will immediately indicate to the enemy that something unusual is in the building, particularly if he is employing comparative surveillance techniques.
95. For efficient operation it may be desirable to stack stores in regular patterns. However, this will not assist in concealment and a compromise between the requirements of camouflage and efficient operation will have to be achieved. In areas where there is a lack of overhead cover, camouflage nets or a screen may have to be erected to give covered storage and working space. There are two requirements for such overhead cover:
- a. The screen must give sufficient cover to conceal movement and the shadows of objects beneath it.
 - b. The screen in itself must produce a surface which matches the background in tone and colour. The tone, as far as aerial imagery is concerned, is decided by the texture of the surface, ie its shadow content as visible from the air. At one end of the scale is the smooth concrete surface with no shadows and so ap-

pearing white. Then, appearing progressively darker, come spoil from excavations, plough, young corn, grass, broad-leaved trees, and lastly, gorse and heather whose leaves are too small to mask any of the shadows below. The matching of colour must be watched continuously, and touching-up and replacement of garnishing carried out to keep pace with the seasonal changes of the background.

96. To reduce the risk of shallow drapes and sloping screens on flat ground being betrayed by their shadows when the sun is low, the angle with the ground should not exceed 15 degrees. The risk can be avoided altogether if the site is chosen so that the cover butts against a hedge or the edge of a wood into which the shadow can fall. Remember that if vertical "walls" are combined with a fully garnished flat top, the result will appear from the air as a solid shape. In undulating ground, the shape of the cover must be planned so that it throws shadows that are similar to the shadows thrown by natural ground features.
97. Flat tops should be extended to fit into the background pattern so as to facilitate concealment of perimeter posts and supporting wires. Walls, hedges and fences are useful and in parkland a judiciously selected line of trees can be used as perimeter posts. There have to be enough supporting wires to prevent the nets or screens sagging so that unnatural shadows are cast. The normal minimum interval between wires is 1 metre.



Stores dispersed along a tree line

98. For temporary stores dumps and replenishment points adequate concealment can normally be obtained by careful siting. Care should be taken however not to over-estimate the cover given by trees; coverings will be required to prevent shine from metallic containers. Where a suitable roadside ditch or hedge exists, it allows an even

distribution of stores along its length without creating fresh tracks. Select the side which is most accessible and, preferably, where the stores will be in shadow most of the day. Where possible however, full use should always be made of cover away from the roadway itself. It is probable that the dumped stores will be seen from the air by a pilot following the road.

Installations

99. Countersurveillance has to be considered when planning new installations. The greatest care should be taken in construction to disturb the surroundings as little as possible and the resiting of potential targets by only a few feet may have a major effect on concealment. Good design and the careful choice of construction materials is essential if the installation is to blend with its environment. No amount of work after completion of construction will ever fully compensate for lack of forethought and planning.
100. The toning down phase can include the painting or surfacing of buildings, roads, etc in a natural colour, planting trees to break up the outline of buildings and the irregular mowing of grass to match the surrounding field pattern. The aim of the deception phase is to distort the appearance of the installation so that it will be more difficult for the attacker to recognize it, especially if he has been briefed from pictures taken before the outbreak of hostilities. The measures taken could include the erection of decoy buildings, painting in contrasting colours, and the demolition of redundant buildings or prominent landmarks in the vicinity of the installation. If it is considered that heat seeking missiles could form part of the attack, decoy heat sources should be displayed.

CHAPTER 4

CAMOUFLAGE IN SPECIFIC ENVIRONMENTS

SECTION 1 - COLD WEATHER CONDITIONS

Snow Covered Terrain

1. Harsh cold weather conditions, whether snow covered or not, provide extra challenges to achieving successful camouflage and concealment. In addition to the changes which occur to local colour, the still air carries noise and vapours much greater distances. The effects of cold weather may well sap the energy and enthusiasm of soldiers, so commanders will have to pay particular attention to ensuring that all basic military disciplines, including camouflage and concealment, are carried out.
2. To achieve camouflage and concealment, the individual should always try to copy nature and blend in with his surroundings as much as possible. In operations where snow covers the ground, the whiteness of the countryside emphasizes any item which does not blend in naturally with its surroundings. Every movement leaves clearly defined tracks. Backgrounds are continually changing and although white is the predominant colour, the texture of the white materials used for camouflage should also be considered. The following paragraphs outline the main points.

Individual Concealment

3. ***Clothing.*** Although the terrain over which operations are carried out varies considerably as far as cover is concerned, it can be classified into four basic types. The types and recommended clothing combination for each type are shown below, although soldiers should always be prepared to change their camouflage as they move from one type of terrain to another.
 - a. *Heavily Forested Areas.* These consist mainly of coniferous trees, or dense deciduous trees with thick under-brush and willows; all dark, disruptive patterned, clothing is best.
 - b. *Low Patchy Bush or Light Scrub Areas.* These are mostly found in hilly or rolling country of poor soil where open snow background predominates. A combination of dark trousers and white jacket is generally the most suitable.
 - c. *Open Snow Covered Areas with Dark Woods and Scrub in the Background.* These are found in hilly or mountainous regions. White trousers and dark jacket are generally the best combination.
 - d. *Open Snow.* All white clothing is the most suitable, but care must be exercised in ensuring weapons and accoutrements are similarly camouflaged.

4. ***Movement.*** Before any move of his force, a commander has to make a careful study of his proposed route, task and time available and arrange for the correct clothing combination to be worn.

Concealment of Equipment

5. Small items of equipment and weapons are relatively easy to camouflage with excellent results being achieved by the use of matt white paint and white adhesive tape. Larger items such as tents and vehicles require more consideration. Generally the quickest method of camouflaging a large object is to make use of a snow camouflage net in conjunction with natural vegetation. Care should be taken not to disturb the snow cover on vegetation being cut. Particular attention should be paid to breaking up the silhouette of the object concerned and to avoiding the creation of prominent shadows. Vehicles should be painted in black and white disruptive pattern; the best results will be obtained by overpainting the areas which are usually painted green with white.



Snow Camouflage

Concealment of Field Defences

6. All field defences have to be camouflaged whether they are dug down into the snow, or built up above the snow level. Where possible they should be sited under the overhead cover of the surrounding trees and brush. The following points should be noted:
 - a. The sides and ends of all trenches should have pronounced slopes and rounded edges to prevent the formation of shadows.

- b. Do not dig to ground level as dead grass, twigs, leaves, etc, mixed with the excavated snow make a sharp contrast with the surroundings and the bottom of the fortification becomes obvious. If this is unavoidable, break up the regular pattern by adding twigs, branches, or trees.
- c. Troops walking back and forth will pack the snow in the bottom of trenches and discolour it. Fresh snow must be added from time to time.
- d. Snow spoil from all excavations should be brushed smooth with twigs or boughs and not left lumpy or in uneven piles.

Track Discipline

- 7. Tracks are extremely difficult to conceal. The only effective method is strict track discipline and the use of deceptive tracks. Tracks can be partially concealed from air observation by breaking up the sharp edges that cast shadows. This can be achieved by trailing large trees behind each track of vehicles. Alternatively, tracks can be extended to logical destinations with the vehicles concealed before that destination. In certain areas, with little or no natural cover, it is worth considering covering the position and adjoining grid squares with tracks.



Track Discipline ?

Light Discipline

- 8. During cold weather operations, the hours of darkness are usually long. Troops have to be trained to accomplish the majority of their tasks without the use of light. Light reflection from the snow and vapour in the air can be seen from great distances, especially on clear cold nights.

Vapour Discipline

9. In very cold still air local fogs or vapour clouds form above anything that gives off heat such as vehicle exhausts, firing of weapons, and the natural heat given off by a man in breathing. In some instances these fogs can be minimized but when conditions remain constant, the only solution may be to move. Vehicles should be left in rear areas, depending on the severity of the conditions. Troops should breathe through their balaclava or headover. Alternatively, they can obtain white surgical masks to breathe through.

Noise Level

10. In still cold air sounds travel longer distances. Conversations can be heard up to a mile away, while the cocking of a weapon can be heard at half a mile. Troops need to be constantly reminded about silence and keeping noise to a minimum. Orders have to be given quietly and where possible, all the activities of daily living kept to inside vehicles or shelters, which assist in muffling sounds. Movement should be kept to an absolute minimum.

SECTION 2 - DESERT ENVIRONMENTS

11. ***Terrain.*** Desert is defined as those hot weather areas consisting primarily of sand dunes, which may vary in height from a few to several hundred feet, or of flat gravel plains. Such areas frequently include or lie adjacent to areas of rugged and barren mountains. In some areas long lines of sight will allow surveillance devices to be particularly effective. Scattered and stunted trees, usually thorns, may be found in certain desert areas, as well as low bushes which may be seasonal and appear only after rains. Nevertheless a primary characteristic of these areas is the absence of vegetation which could provide overhead cover. The principles of camouflage and concealment do not change in the desert. Particular imagination and ingenuity is, however, required in their application if the inherent difficulties of concealment in the desert are to be overcome. For instance, if the situation allows and communications are good enough, it may be best to disperse for countersurveillance and regroup for action.
12. ***Special Considerations.*** Four features of countersurveillance activity need to be highlighted for desert operations. They are:
 - a. ***Movement.*** Vehicle dust clouds may be seen at very great distances, particularly from the air. Good choice of ground, the avoidance of "tracking" by drivers, and the reduction of speed can all help to reduce dust clouds. The creation of new tracks must also be avoided wherever possible. Heat haze may also offer some cover but temperatures may be so high as to make movement undesirable in daytime. Haze and dust clouds in late afternoon may make this a better time of day to carry out digging, wiring, replenishment etc than cold clear nights when all surveillance devices perform better.
 - b. ***Colouring.*** Background colours vary considerably and include various shades of grey, red, brown and yellow. Service camouflage nets rarely match these

colours and often stand out. This problem may be overcome by the disruptive painting of vehicles and by painting or dyeing camouflage nets and clothing in the locally prevalent colours.



The problems of concealment in the desert

- c. *Shadow.* Very harsh shadows are thrown, and this problem is made worse by the sparsity of natural shade or overhead cover. Where no natural shade exists, care must be taken to ensure that camouflage nets cover the shadow thrown by a vehicle or piece of equipment as well as the equipment itself.
- d. *Deception.* Due to lack of cover it may often be impossible to achieve total concealment. In such cases deception by disguising vehicles and equipment as the huts of local inhabitants, or by disguising attractive targets, have frequently been successful. The construction of dummy positions is relatively easy and often proves well worthwhile by focussing the attention of observers and attackers on the wrong area.

SECTION 3 - MOUNTAIN ENVIRONMENTS

- 13. The principles of countersurveillance described earlier are also true for mountainous environments. Concealment, however, is made more difficult as:
 - a. Terrain and vegetation may alter radically, depending on the altitude at which operations are being carried out. At high altitudes, natural cover will be limited.
 - b. Movement is generally restricted to paths and trails which normally follow valley bottoms or ridge lines. These allow an enemy to concentrate his surveillance sources, instead of dispersing them over wide areas.

- c. An enemy will take every opportunity to establish observation posts on high ground, where good fields of view are available.

14. Concealment of movement needs to be based on:

- a. Moving bodies of troops at well spaced intervals. Movement should never take place on ridge lines; troops should move just under the crest of a spur with only limited numbers in such a position that they can watch the reverse side of the slope.
- b. Making the maximum use of the heavy cast shadows, caused by surrounding high features.
- c. Making the best use of dead ground.

15. For individual concealment and the concealment of field defences, natural cover should be improved as opportunity offers. However, piles of small stones and sangars, unless they have been properly constructed by our own troops, should be avoided. They are seldom bullet-proof and are often used as aiming marks by the enemy. The digging of field defences will often not be possible owing to the nature of the ground. Troops in position have to keep as motionless as possible; there should be no unnecessary movement.

SECTION 4 - JUNGLE ENVIRONMENTS

16. Countersurveillance activity is also valid in jungle conditions. Concealment is made easier because:

- a. The dense vegetation provides good cover.
- b. There is intense contrast between the bright reflections in tropical sunlight and deep shadows.
- c. Ground observation is seldom possible beyond 50m and may be reduced to as little as 2m in swamp or secondary growth.
- d. Air to ground observation, which is generally restricted by jungle vegetation canopies, is often further limited by mist, fog, low cloud, heat haze and rain which can persist for several days.



Visibility is a few metres in the Jungle

17. A trained observer will look for:
 - a. Boot marks on tracks, leaves unnaturally turned, bruised or bleeding roots, and freshly cut saplings muddled over at ground level.
 - b. Warm ash on an "old" fire.
 - c. Dry patches on the ground after rain.
 - d. Unnatural litter.
 - e. Disturbed insect life and broken spider webs across a track.
18. Hearing and smell will supplement the information an observer gains by visual observation. For example, the smell of cigarette smoke can be detected a considerable distance away from the smoker, as can cooker fuel, any sort of scented soap or even human sweat. The noise made by machetes cutting down saplings to make "bashas" can easily give away a well concealed position. A high degree of personal camouflage, good basic soldiering skills and a high level of personal discipline are essential in jungle operations.
19. Vehicle movement through jungle is difficult and almost all vehicle traffic remains on formed roads and tracks. Aerial observation of roads can be made more difficult due to the jungle canopy. However, the principles of detection (shape, shadow, shine etc) still apply. Any disturbance to the jungle canopy such as gaps, unnatural movement and patterns are quickly identified by observers. Smoke and straight lines of angular shapes are also highlighted in this environment.

CHAPTER 5

COUNTERSURVEILLANCE TRAINING AT UNIT LEVEL

SECTION 1 - TRAINING

1. The training of soldiers in the art of countersurveillance is both challenging and rewarding. It is a subject which is not easy to bring alive and make interesting. Training in a peacetime environment, lacking the necessary incentives of wartime conditions, make it difficult for the individual to appreciate the implications of the surveillance threat.
2. Countersurveillance is not a natural skill. It has to be taught and practised regularly so that a high standard is achieved and maintained.
3. Only by having a true awareness of a threat can unit training be effective. All ranks have to realize that surveillance devices which are likely to be employed have their limitations and it is on these limitations that countermeasures need to be focussed. The camouflage and concealment of a unit, though becoming more challenging, is by no means impossible.
4. Within the unit, the importance of countersurveillance techniques should be emphasized to:
 - a. *Commanders at All Levels.* In particular, those who will be responsible for selecting routes, harbour areas, work sites or defensive locations.
 - b. *Drivers of All Vehicles and Equipment.* It only requires the careless camouflage of a single vehicle to give away a unit location.
5. All arms training and advice on countersurveillance is the responsibility of the Surveillance, Target Acquisition, Night Observation and Countersurveillance (STANOC) Centre at Larkhill, where regular courses for unit instructors in the subject are held. It is important, however, that countersurveillance should become as natural a part of routine unit training, as any other subject. The following points may help to stimulate the interest of soldiers and increase their awareness of the problems involved:
 - a. Where possible, aerial imagery of unit exercises should be obtained. The results of such photography should be circulated on a wide distribution within the unit, together with comments on the success or otherwise of the camouflage achieved.
 - b. Helicopters should be incorporated into suitable unit "work-up" exercises with a view to affording junior ranks the opportunity of viewing camouflaged positions from the air. The impressions gained from an aerial view will differ considerably from those obtained on the ground.
 - c. Where items of surveillance equipment such as Spyglass or OTIS are held within units, these should regularly be deployed to test the effectiveness of the countermeasures used.

- d. Practice should be given in the use of simple deception techniques.
 - e. Adequate stores and equipment have to be available to enable those involved in countersurveillance training to undertake their tasks efficiently.
 - f. Obvious tactical markings should be kept as small as possible. This applies both to vehicle markings and route direction markers.
6. Countersurveillance training needs to be regarded as the responsibility of all within a unit; there can be no exceptions. If one part of the unit is allowed to regard itself as free from this responsibility, a poor overall standard will result. Commanders at all levels should ensure that countersurveillance discipline is maintained at all times.

SECTION 2 - PREPARATION AND SELF HELP

7. There are several artificial aids which are available for use by the individual to help him to conceal himself. These are:
- a. *Helmet Net and Cover.* The combat helmet should always be kept covered with the issue camouflage cover. Garnishing should be added to match the background.
 - b. *Camouflage Face Cream.* This should be applied in a disruptive pattern to all exposed areas of skin.
 - c. *The Face Veil.* This can be used to conceal the outline of the head, shoulders and webbing equipment.
 - d. *Individual Camouflage Net.* This is an issue to some specialist forces. It is a lightweight, robust and extremely effective piece of equipment.

SECTION 3 - EQUIPMENT

Materials

8. ***Urban Camouflage Material (UCM).*** UCM is a replacement for hessian, for use as urban camouflage. It is available in 3.5 m x 60 m rolls in grey and brown. Details are:
- a. Cloth Woven Polypropylene (UCM) Grey (Rolls)
H5/8305-99-799-3130.
 - b. Cloth Woven Polypropylene (UCM) Brown (Rolls)
H5/8305-99-799-3131.
 - c. Eyeletting Kits (25 eyelets)
H5/5325-99-799-3132.

9. ***Thermal Camouflage Material.*** Two versions, Thermal Camouflage Woodland (TCW) and Thermal Camouflage Arctic (TCA) are now in service.
10. ***Hessian or Camouflage Drape Material (CCSOD).*** Preferably dark in colour, these are required to cover all reflecting surfaces and drape over areas of contained shadow. CCSOD has replaced hessian for this purpose. To assist in the rapid concealment of the reflecting surface and the contained shadows on vehicles, prepositioned CCSOD can be used. CCSOD drapes can be simply manufactured through unit resources.

Support Systems

11. ***Camouflage Support System (CASS).*** CASS is an equipment based on flexible fibreglass rods, to replace conventional methods of supporting camouflage nets. It is issued as part of the concealment sets for all high value equipments.
 - a. ***Paints.*** Guidance on pattern painting of vehicles is given in Materiel Regulations for the Army Volume 2 - Equipment Support, Pamphlet 4 - Equipment Support Repair Procedure Section 5 - External Painting of Army Vehicles. Vehicles and Technical Equipment Pamphlet No 3 - Painting of Army Vehicles, Aircraft and Equipment (Army Code 60503 Pamphlet 3) dated October 1988. Paints available are:
 - (1) Paint Finishing Spraying NATO Green (IRR)
HI-8010-99-224-8906.
 - (2) Paint Finishing Brushing NATO Green (IRR)
HI-8010-99-224-8907.
 - (3) Paint Finishing Brushing Black
HI-8010-99-224-8908.
 - (4) Paint Finishing Emulsion for Canvas NATO Green (IRR)
HI-8010-99-225-0094.
 - (5) Paint Finishing Emulsion for Canvas Black
HI-8010-99-224-4891.
 - (6) Paint Emulsion Finishing Brushing White
HI-8010-99-224-4894.
 - (7) Paint Emulsion Heat Resisting Brushing White
HI-8010-99-225-1791.
 - (8) Thinner (for all except emulsions)
HI-8010-99-942-8846.
 - (9) Paint Finishing Temporary Snow Camouflage
HI-8010-99-894-0112.

- b. *Camouflage Creams.* The individual camouflage cream pack (HI-6850-99-978-5980) may be used.
- c. *Camouflage Nets.* Information on NATO stock numbers and net sizes for vehicles and equipment is contained in The Catalogue of Ordnance Stores and Ammunition Section H5 - Camouflage Equipment (Army Code No 14283).
 - (1) *Desert Net.* This is for use in mainly sandy areas. It consists of a polyester lace garnishing material covering a 200 millimetre mesh hemp net.
 - (2) *Snow Net.* This is made of spun nylon netting garnished with incised acrylic coated nylon.
 - (3) *The Mark 5 Woodland Net.* This is for use in all green, or partly green areas. It comprises spun nylon netting garnished with incised polyurethane coated nylon patches.
 - (4) *The Mark 7 Woodland Net.* Issued as a replacement for the Mark 5 net.
 - (5) *Moorland/Woodland Net.* This net has moorland camouflage on one side and woodland camouflage on the other side. It is primarily for use on the Southern Flank of NATO and in the Falkland Islands.

Accessories

- 12. To obtain the most effective camouflage against detection in both the visible and infra-red bands, the following equipment accessories should be available for use in conjunction with the relevant camouflage net at all times. It is recommended that they form a normal part of vehicle equipment:
 - a. *Poles or Props.* Sufficient numbers of these should be carried on the vehicle to avoid the necessity of the driver having to cut more on his arrival in a harbour area.
 - b. *"Mushrooms".* These should be carried so that when used in conjunction with a net prop, sharp points on the camouflage netting can be avoided. Other designs are currently under development.
 - c. *Pegs.* These are issued as part of concealment sets. For units without concealment sets, they should be locally produced or procured, to peg down the edges of camouflage nets.

Maintenance of Camouflage Nets

- 13. After use, all types of nets should be dried, correctly folded and any foliage removed. When in store they should be inspected at least once every three months and any necessary repairs effected. After a period of use a net will require regarnishing which is a unit responsibility.

SECTION 4 - THE STANOC CENTRE

14. The STANOC Centre, as well as advising on surveillance and countersurveillance matters, runs courses to train unit instructors from Sgt to Maj on all aspects of modern countersurveillance techniques. Information on these courses is available from:

The STANOC Centre
Larkhill
SALISBURY
Wiltshire SP4 8QT

Signal Message Address:

STANOC LARKHILL

Telephone numbers:

S02(W) Countersurveillance	Larkhill Military 5679
QMSI Countersurveillance	Larkhill Military 5272
Clerk	Larkhill Military 5283
Fax	Larkhill Military 5785

PART B

OPSEC

CHAPTER 1

BACKGROUND TO OPSEC

SECTION 1 - THE OPERATIONAL ENVIRONMENT

General

1. Operations Security (OPSEC) is defined as: the process which gives a military operation or exercise appropriate security, using passive or active means, to deny the adversary knowledge of the dispositions, capabilities and intentions of friendly forces.¹
2. UK doctrine conforms to the manoeuvrist approach to operations², in which shattering the enemy's overall cohesion and will to fight is paramount. The emphasis is on the defeat and disruption of the enemy - by taking the initiative, and applying constant and unacceptable pressure at the times and places the enemy least expects. A primary consideration for commanders will be the need to get inside the enemy's decision/action cycle; to take the initiative and to pre-empt him at all times. The key to this will be information – in order to make our decisions, we must discover as much as possible about the enemy's dispositions, capabilities, vulnerabilities and intentions. It follows, then, that we must deny the same information on friendly forces to the enemy.
3. Effective countersurveillance is not enough to achieve this. It is impossible to hide completely a major unit, still harder to fully conceal formations with their logistic support. However, although an enemy may be aware of the presence of friendly forces, without detailed knowledge of their dispositions, capabilities and intentions he cannot plan and act effectively. This information is denied to him by the application of the OPSEC process.

OPSEC and Information Operations (INFO OPS)

4. The concept of INFO OPS³ is now widely adopted within NATO. INFO OPS enable the commander to make overall and effective use of military capability and information within a framework of offensive and defensive measures. The overall control and direction of INFO OPS is at the military strategic level. The operational level activity forming part of INFO OPS is Command and Control Warfare (C2W)⁴, which includes

1. AAP-6.

2. British Defence Doctrine, JWP 0-01.

3. Defined as actions taken to influence decision makers in support of political and military objectives by affecting others' information, information based processes, Command and Control (C2) systems and CIS while exploiting and protecting one's own information and/or information systems. There are 2 main categories of INFO OPS: defensive INFO OPS and offensive INFO OPS, depending on the nature of the actions involved.

4. The integrated use of all military capabilities including Physical Destruction, Electronic Warfare, Deception, Psychological Operations, and Operations Security, supported by All-Source intelligence and CIS, to deny information, to exploit, influence, degrade, confuse or destroy enemy C2 capabilities and to protect friendly C2, intelligence and CIS against such actions.

OPSEC and deception. While both are military disciplines in their own right, and can be applied in isolation, the best results will be achieved when both are used as part of a co-ordinated C2W plan.

SECTION 2 - CONCEPT OF OPSEC

5. OPSEC addresses the overall security of an operation, in the light of an enemy's known or suspected Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) capabilities. Each operation is examined in its entirety from an enemy's viewpoint, including: land, sea, air and rear area activity; lines of communication, and all Communications and Information Systems (CIS) networks, in order to identify those indicators from which an enemy could deduce information about an organisation, operation or exercise. These indicators are then given the appropriate protection in order to deny an enemy knowledge of the dispositions, capabilities and intentions of friendly forces. Intelligence that the enemy may already have from other sources should also be considered.
6. An OPSEC plan can only be brought about by the co-ordinated effort of commanders and their personnel, and through the use of a combination of OPSEC measures. OPSEC is equally applicable to exercises, rehearsals and other preparations, and at all levels, from Force through to unit.
7. The basis of OPSEC is that, as it is not possible to conceal every military action in support of an operation, it concentrates on those critical activities which could indicate the existence of an organisation, impending operation, or its details, and thereby reveal intentions, capabilities and potential vulnerabilities. These aspects or indicators are called Essential Elements of Friendly Information (EEFI).
8. OPSEC is not a process to ensure protection of all information or to completely hide an operation or the forces involved. A balance of risk is inevitable. Unduly oppressive OPSEC runs the risk of being counter-productive in terms of resource costs and limitations on friendly activity. Conversely, relaxed OPSEC allows greater freedom of action but increases the risk of compromise.
9. There is a relationship between OPSEC and deception. OPSEC aims to prevent an enemy from identifying friendly dispositions, capabilities and intentions, whereas deception aims deliberately to present a false picture. An OPSEC plan need not, therefore, include deception: conversely a deception plan must include OPSEC to hide the reality and assist in presenting a false picture to the enemy. Thus there is a synergy between OPSEC and deception: while OPSEC denies information to an enemy, deception fills that void with information tailored for his consumption.

CHAPTER 2

THE PROCESS AND EVALUATION OF OPSEC

SECTION 1 – PRINCIPLES OF OPSEC

Principles

1. **Enemy's Viewpoint.** OPSEC assessments have to be conducted from the point of view of an enemy. The key to identifying critical information is to determine what can be deduced from a particular event or piece of information, hence the importance of identifying and protecting EEFI. Where there is more than one enemy, care must be taken to conduct an assessment from each of point of view as the value of an EEFI may vary from one enemy to another.
2. **Critical Information.** OPSEC assessments should identify those critical events, activities and equipment that an enemy can use to predict, disrupt or defeat a friendly operation.
3. **Highest Level.** The OPSEC plan needs to be co-ordinated at the highest level of command involved in an operation. Distribution of OPSEC assessment results should be restricted to the commander of the operation and key members of his staff on a "need to know" basis, as general dissemination could result in individual units taking their own OPSEC measures independently, to the detriment of the overall plan.
4. **Comprehensiveness.** OPSEC should address all aspects of an operation. These include timings, administration, logistics, communications and movement, for all elements of the force.
5. **Timeliness.** Assessments of vulnerability have to be made before, or during, operation/exercise planning. They must continuously be revised as developments occur, to pre-empt new threats. OPSEC cannot be successfully imposed after an event as it is difficult to determine what may have been compromised, and thus to decide on which appropriate measures need to be implemented.
6. **Appropriateness.** An accurate assessment of both friendly indicators and the enemy's ISTAR capabilities is necessary. Measures need to be appropriate to the operation; countering an exaggerated capability can divert scarce assets from the operation itself.
7. **Acceptability.** OPSEC measures should appear to an enemy to be part of normal operations. They should not in themselves draw the enemy's attention. OPSEC measures may be part of a Deception Plan but, if necessary, deception measures may need to be incorporated into the OPSEC plan to disguise certain OPSEC measures.
8. **Flexibility.** The OPSEC plan is to be capable of change at very short notice, and should be continuously reviewed to take account of events. The plan should include

contingency elements to cover developments as the operation proceeds, and for counter-compromise action.

9. **Systems Analysis.** OPSEC systematically examines the security of entire operations or phases of an operation. Static or isolated installations, documents, equipment and/or events are only included in the OPSEC plan when they themselves form, or contribute to, EEFI. Otherwise they are addressed by standing security measures.

SECTION 2 - THE OPSEC PROCESS

Stage 1 - Identification of Critical Information

10. **Preliminary Assessment.** The Intelligence Preparation of the Battlefield (IPB) should include an outline assessment of an enemy's ISTAR capabilities, both within and outside of the area of operations. This also includes the ISTAR capability of an enemy's allies and the threat from espionage, subversion and terrorism.
11. **The Estimate.** This assessment of an enemy's ISTAR guides the Commander in his Estimate as to what general activities the enemy is likely to detect. The Commander includes OPSEC as a factor in his Estimate and provides guidance to his staff as to which aspects of his plan or exercise can or should be disclosed as a contribution to deterrence or deception, and which aspects must be protected. As with his intelligence requirements, these may be specifically stated as the Commander's OPSEC requirements.
12. **Identify EEFI.** The G2 staff, in conjunction with G3, identifies the EEFI within the Commander's plan. This process will also identify the specific indicators, eg key vehicles/equipments and activities within these EEFI. Examples of EEFI are given at Annex A.
13. **OPSEC Estimate.** A separate OPSEC Estimate may need to be prepared for major or critical operations. The OPSEC Estimate should follow on from the Commander's Estimate, as the Commander's chosen Course of Action (COA) and the resultant EEFI's will drive the selection of OPSEC measures. A possible format for the OPSEC estimate is at Annex B. Amongst other considerations, the estimate will need to identify those activities that threaten to expose friendly force vulnerabilities. In this respect, it should cover:
 - a. An enemy's ISTAR capabilities.
 - b. Mapping an enemy's ISTAR capabilities against similar friendly systems, highlighting vulnerabilities and commissioning remedial action, if and where necessary.

Stage 2 - Analysis of Threats

14. Having identified the EEFI and their associated key equipments and activities, G2 staff can assess in detail:

- a. What the enemy is already likely to know or to have deduced, given his perceived collection capability.
- b. The enemy's capability to detect the EEFI.

Stage 3 - Analysis of Vulnerabilities

15. Possible OPSEC measures are identified to protect the EEFI following the analysis of threats. The most desirable measures provide the necessary level of protection at the least cost to operational efficiency. OPSEC measures fall under five broad categories:
- a. *Defensive Measures.* The aim of defensive measures is to counter the enemy's ISTAR assets.
 - b. *Active Measures.* The aim of active measures is to disrupt or destroy the adversary's ISTAR capability. This can include Electronic Countermeasures (ECM), Counter-Intelligence (CI) and physical destruction.
 - c. *Deception.* Deception aims to mislead an enemy's command staffs. A deception plan, limited to covering an EEFI that cannot otherwise be concealed (eg the movement of a formation across open ground) may be needed.
 - d. *Presentation of Measures.* Consideration should be given, prior to and during operations, to the scope for influencing an enemy's perception of OPSEC measures, thus disguising their aim. For example, the destruction of a key enemy ISTAR asset could be combined with a wider attack, concealing the real objective.
 - e. *Change of Plan.* Friendly plans can be changed if part of the operation is compromised (timings of moves, locations, units, etc).

Stage 4 - Selection of OPSEC Measures

16. The selection of OPSEC measures is conducted in three stages:
- a. *Determine Impact.* G3 analyses:
 - (1) The impact of an OPSEC measure on operational efficiency.
 - (2) The probable risk to the operation's success if the measure is not implemented or is unsuccessful.
 - (3) The resource implications of implementing OPSEC measures.
 - b. *Determine Protection.* With specialist advice (see Annex A), and taking into consideration factors such as ground, weather, local population and media activity, G3 staff determine what should be protected and what may remain unprotected (and at what risk).

- c. *Interaction of OPSEC Measures.* The appropriate OPSEC measures are determined in conjunction with G2 staff and other specialists, and approved by the Commander. The interaction of the OPSEC measures is checked to ensure that protection of one piece of critical information does not unwittingly compromise another. Before giving his final approval, the Commander should be briefed on the proposed OPSEC measures and any operational penalties they may incur. Where protection is not possible, or where information may already have been compromised, changes to the plan or deception measures may be initiated, or the risk accepted. Some information may be deliberately disclosed if it supports a deception plan and does not jeopardise the operation.
17. ***Application of OPSEC Measures.*** The OPSEC plan is normally produced as an Annex to the Operation Plan, although key measures (such as the OPSEC objectives and Emission Control [EMCON]) may be incorporated in the main body of the order. Monitoring and reporting procedures for OPSEC breaches should be included in the plan. The OPSEC plan may need to be produced and distributed as a series of separate appendices for security reasons.
18. ***Responsibilities.*** The implementation of measures in accordance with the OPSEC plan is the responsibility of all commanders. At Divisional level and above dedicated OPSEC staff should be appointed to co-ordinate the OPSEC plan.
19. ***Evaluation.*** The OPSEC plan is continuously re-evaluated by G2 and G3 staffs as the operation progresses, consulting other staffs as appropriate. As the operation progresses, certain OPSEC measures may become irrelevant and can be lifted. G2 monitors intelligence input to determine the effect of OPSEC measures. The OPSEC staff act as the central monitoring and reporting point for OPSEC, and may task friendly assets to monitor the OPSEC plan, eg for communications security (COMSEC) breaches. SIGINT, EW and HUMINT elements can monitor the effects of OPSEC measures. Specialist teams can be tasked specifically if required.
20. ***Suspected Failure of an OPSEC Measure.*** Whenever the failure of an OPSEC measure is suspected the Commander/G3 staff have to be informed to allow consideration for modifications to the plan. G3 reviews the OPSEC plan as the commander's priorities change, or when an OPSEC measure fails. The following factors should be considered:
- a. Developments in the enemy's ISTAR capability.
 - b. Disclosures by PWs, neutrals, or the media.
 - c. Breaches of security/disclosures by friendly forces.
 - d. The stage of the operation - are one or more of the protagonists irrevocably committed to a particular course of action?
 - e. If the adversary becomes aware of the operation's details, does he have the ability to influence its course at that stage?
21. ***Protection of OPSEC Evaluation.*** Distribution of OPSEC evaluation results should be restricted to prevent compromise. Lessons learned from evaluation of OPSEC should be incorporated into future OPSEC planning.

EXAMPLES OF ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI)

EEFI will vary considerably according to tactics, type of force involved (armoured/mechanised/light infantry/combat support), objectives, terrain, obstacles, etc. The EEFI given below are for illustrative purposes only. Note that the indications in column (c) would be deduced from an enemy's analysis of a number of EEFI and his knowledge of the overall situation, rather than from a single EEFI in isolation.

EEFI	Specific Indicators (signature vehs and activities)	Typically Indicative of
(a)	(b)	(c)
BG O Gp.	Inf, Armd and Arty Comd Vehs.	Movement; precursor to activity.
Reinforcement.	Additional personnel/vehs.	Offensive action.
Reduced manning/ equipment in unit location.	Move of vehs; fewer personnel and vehicles in location.	Withdrawal/relocation.
Combat resupply.	Fuel bowzers; ammunition vehicles.	Offensive action; precursor to activity.
Rehearsals.	Various.	Intentions.
Armd recce.	Recce vehicles.	Intentions and routes; objectives.
UAV flights.	Phoenix.	Intentions and routes; objectives.
Engr obstacle crossing activity.	Armd bridgelayers; bridging equipment; minefield breaching equipment.	Intentions and routes.
Minelaying.	Minelaying vehicles.	Adopting defensive posture.
Stockpiling Engr stores.	Wheeled vehicles; Engr stores.	Intentions; precursor to activity.

EEFI	Specific Indicators (signature vehs and activities)	Typically Indicative of
(a)	(b)	(c)
Pre-positioned artillery ammunition.	DROPS vehicles; stacks.	Offensive action.
Artillery OP activity.	Move forward of OP vehicles.	Intentions; precursor to activity.
Comms activity on Arty net.	Increased activity detected by enemy ESM.	Precursor to activity.
Increased AD activity.	Radars active; move of Rapier equipment.	Air routes and ground movement areas - intentions; movement; precursor to activity.
Reconfigure Combat Net Radio.	Movement of Rebro stations and SCRA Centrals; changed level of activity detected by enemy ESM.	Movement; precursor to activity.
Establishing Forward Ammunition and Refuelling Point (FARP).	Kerosene bowzers; re-arming vehicles.	Main effort; intentions and objectives.
Marrying ground and aviation elements.	Dismounted troops near open space; helicopters landing.	Precursor to air manoeuvre operations - main effort; intentions; objectives.

FORMAT FOR THE OPSEC ESTIMATE

During rapidly moving operations an OPSEC Estimate is likely to take the form of a swift mental appraisal made with the help of a map and supplemented by hasty notes. But, so far as possible, this mental appraisal should follow the suggested sequence for a Full Estimate. Where possible, the OPSEC Estimate should be conducted after the Commander's Estimate to avoid nugatory work and ensure that all aspects of the proposed COA are covered.

Likely OPSEC Mission	To deny enemy knowledge of (Unit/Formation name) preparations for
(a)	(b)
Factors (derived from IPB).	<i>Enemy</i> a. Assessed extent of enemy knowledge of friendly forces. b. Threat from current enemy surveillance activity. To cover all ISTAR assets. c. Threat from sabotage, subversion and terrorism. Consider Special Forces and laser target markers. <i>Environment</i> d. <i>Terrain</i>. Effect on enemy ISTAR and own OPSEC measures. e. <i>Weather</i>. Effect on enemy ISTAR and OPSEC measures. f. <i>Local Population</i>. Presence in Area of Operations (AO); friendly or hostile. g. <i>Media</i>. Extent of media interest and presence in AO. <i>Time</i> h. <i>Time and space</i>. Effect on enemy ISTAR and own OPSEC measures. Timeliness of enemy command system and ISTAR assets.

(a)	(b)
	<i>Friendly Forces Plan</i> i. Intentions, objectives, methods, flanking formations, vulnerabilities. j. Identify EEFI and consequent critical information arranged in order of importance to cover such areas as: (1) Movements. (2) Logistics. (3) Communications and Information Systems (CIS). (4) Personalities. (5) Morale. k. Equipment. l. Assessment of enemy knowledge. m. Other factors.
Assessment of own vulnerabilities to enemy ISTAR.	
Assessment of OPSEC Measures.	a. Defensive. b. Active, including destruction of ISTAR systems where countermeasures are not possible. c. Deception. d. Presentation. e. Change of Plan.
Consideration of COA.	a. Description. b. Advantages. c. Disadvantages/Vulnerabilities.
Selection of Optimum COA.	
Produce OPSEC Plan.	
Review plan as operation develops.	

CHAPTER 3

OPSEC MEASURES

SECTION 1 - GENERAL POINTS

1. The OPSEC plan will normally consist of a number of Force-wide measures, together with specific measures (often imposed for a limited period only) for individual units, equipments, installations or areas. The measures selected will be governed by the requirement of each aspect or indicator and whether it needs to be protected or controlled.
2. To ensure a systematic and thorough review, OPSEC measures should be considered under the headings below. A more detailed list of OPSEC measures is at Annex A. They should be assessed against the anticipated threat from an enemy's (or his allies') ISTAR capability, as well as the physical threat from Special Forces, agents and sympathisers.

SECTION 2 - DEFENSIVE MEASURES

3. **General.** Defensive measures aim to counter the enemy's ISTAR assets. They are applicable to all elements of a force. Their imposition will not normally require diversion of significant resources from other tasks.
4. **Personnel Security.** Personnel security covers the risk to individuals from subversion and terrorism, and includes controls to limit movement (curfews, out-of-bounds areas and guards) and to prevent contact between force personnel and potential enemy sympathisers.
5. **Physical Security.** Physical security covers the physical barriers (locks, walls, wire and fields of fire) to be created to deny access to classified or sensitive documents, equipment, military bases and sensitive areas, and to defeat/prevent physical attack.
6. **Document Security.** All documents should be protected in accordance with their classification. Distribution of documents containing EEFI should be limited to those with a need to know, and delivery means assessed for risk.
7. **Electronic Security.** Electronic security covers measures to counter an enemy's EW/SIGINT assets, including:
 - a. *Communications Security (COMSEC).* This includes COMSEC monitoring of friendly communications prior to, and during, operations.
 - b. *Information Security (INFOSEC).* The security of Information Systems (IS), including hardware, software and bearer systems. Particular attention should be paid to IS using commercial bearer systems, such as the Internet. The aggregation of information should also be addressed; several seemingly unimportant pieces of information can add up to a major compromise.

- c. *Electronic Support Measures (ESM)*. These include search, intercept, direction finding and analysis of communications and non-communications transmissions.
 - d. *Electronic Countermeasures (ECM)*. These include jamming, deception and neutralisation of enemy communication systems and his ESM.
- 8. ***Electronic Protective Measures (EPM)***. EPM help to ensure the friendly use of the electro-magnetic spectrum. They include technical features and operating procedures that preserve OPSEC by denying an enemy the opportunity to gain intelligence from friendly use of the spectrum.
 - 9. ***Emissions Control (EMCON)***. EMCON provides selective and controlled use of electro-magnetic, acoustic or other emitters, to optimise command and control while minimising detection and exploitation of an enemy's sensors.
 - 10. ***Camouflage and Concealment***. Camouflage and concealment can assist in defeating surveillance from ground or air. The threat from aerial surveillance platforms must be considered, in particular from satellites. Their orbits and surveillance "windows" should be provided to field commanders from the Force HQ (see Part A, Chapter 1, Paragraph 6).
 - 11. ***Media Security Policy***. Media representatives from the nations involved and from other countries will probably be present in the area of operations during most phases of an operation. They will have access to excellent communications and may be broadcasting "live", their reports are likely to be syndicated worldwide. Although formulation of media security policy is not a tactical concern, its implementation often will be. A media security policy should be formulated at an early stage, certainly prior to deployment, after consultation between Intelligence, Operations, Media Operations and Legal staffs. It should be co-ordinated at Ministry of Defence level to prevent inadvertent disclosures outside the operational area. The media security policy in the area of operations should be directed by the commander, in consultation with the MOD, in accordance with his OPSEC policy.

SECTION 3 - ACTIVE MEASURES

- 12. ***General***. Active measures aim to disrupt or destroy the enemy's ISTAR capability. They are often resource-intensive and will be implemented at battlegroup and formation level.
- 13. ***Air Defence***. Increased AD effort can be directed against Imagery Intelligence (IMINT) platforms.
- 14. ***Military Vigilance***. Increased military activity can be conducted to counter reconnaissance patrols, etc. If an enemy is thought to possess "smart" (terminally guided) munitions then particular attention should be given to sites potentially suitable for enemy teams equipped with Laser Target Markers.

15. **Direct Attack.** Enemy command elements, including intelligence staffs and other intelligence production assets, can be attacked directly (physically and electronically). This will often form part of a wider INFO OPS/C2W plan.

SECTION 4 - OTHER MEASURES

16. **Deception.** At the operational and strategic level, where movements of large formations will occur which cannot be effectively concealed, deception is likely to form an integral part of the OPSEC plan. At the tactical level, duplication of effort can be used to protect EEFI that cannot otherwise be concealed. For instance, recce could be conducted on multiple routes to conceal the intended axis.
17. **Presentation.** Consideration should be given to the way in which friendly moves and intentions are presented publicly, in order to influence an enemy's perception of their importance and purpose.
18. **Change of Plan.** Finally, if other measures have failed or are inappropriate, the plan can be adjusted by changing timings, unit locations, etc.
19. **Compromise or Failure of OPSEC Measures.** If there has been a compromise or failure of an OPSEC measure and countermeasures are not practicable, or no measure can be implemented in time to meet a particular ISTAR threat, then the commander has three choices:
 - a. *Ignore the Compromise.* If the operation has reached the stage when the enemy is unable to influence its course, then the compromise or failure of OPSEC measures can be ignored.
 - b. *Accept the Risk.* If friendly forces are irretrievably committed, or a phase of the operation is vital and cannot be altered, then the commander must accept the risk.
 - c. *Change the Plan.* This might include cancelling, postponing, bringing forward or altering the operation.

USEFUL OPSEC MEASURES

1. **General.** A timely and accurate assessment of friendly indicators will lead to the effective application of a combination of the appropriate OPSEC measures below, both in the initial plan and in the event of compromise.
2. **Defensive Measures to Counter Enemy ISTAR Assets.**
 - a. Personnel Security.
 - (1) Curfews, out-of-bounds areas and guards.
 - (2) Control of personal communications, especially the use of public telephone systems (including mobile telephones), and letters home.
 - (3) Media controls and policy on contacts with media representatives.
 - b. Increased physical security measures.
 - c. Implementation of strict need-to-know policy.
 - d. Countersurveillance measures.
 - e. Noise and light discipline.
 - f. Track/movement discipline.
 - g. COMSEC, EMSEC, INFOSEC and EMCON discipline.
 - h. Movement. Where an enemy's ISTAR assets are limited in number or scope, or lack responsiveness, movement of friendly units and headquarters can overload their capabilities.
 - i. Dispersion. Disperse forces if enemy ISTAR capability limited in size or mobility.
 - j. Use of Terrain. Terrain features can defeat line-of-sight assets and reduce vulnerability to aerial platforms.
 - k. Weather. Fog/mist can frequently be predicted and degrades most ISTAR assets; low cloud reduces aerial threat.
3. **Active OPSEC Measures.**
 - a. Increased patrol activity.
 - b. Increased AD effort to deter or destroy enemy aerial ISTAR.

- c. Direct attack on enemy ISTAR assets, including processing and assessment assets and HQs.
- d. ECM.
- e. Deception to disguise particular phase or deployment of operation.
- f. Arresting/interning suspected enemy agents/sympathisers.
- g. Curfews/out-of-bounds areas to local population.
- h. Use of tactical smoke.

4. ***Change Plan.***

- a. Postpone, stop or move the operation.
- b. Change, alter or modify the plan.
- c. Change, alter or modify operational procedures.

CHAPTER 4

COMMAND AND CONTROL OF OPSEC

SECTION 1 - RESPONSIBILITIES

General

1. OPSEC is the commander's responsibility, and must be co-ordinated throughout the force, from Force down to unit level. This is to ensure a consistent approach and to prevent inadvertent compromise of one unit or formation by another. OPSEC is a G3 function, supported by G2. As OPSEC is one of the components of INFO OPS/C2W it should, where possible, be planned, implemented and monitored by a dedicated cell within the INFO OPS/C2W staff.
2. If no formal C2W structure exists, at formation level and above, a staff component within G3, with the support of other branches, particularly G2, should be specifically responsible for OPSEC, either as a dedicated organisation, or jointly with their other functions. The specific responsibilities of the staff branches in support of OPSEC are covered below. These staffs need to be exercised in OPSEC procedures regularly. The commander's Legal Advisor and Media Ops Advisor should also be involved. As part of the OPSEC staff's function, they should also act as the overall monitoring and reporting point for the OPSEC plan. As part of the wider command process they must:
 - a. Co-ordinate and implement the OPSEC plan within the context of the overall operational plan.
 - b. Co-ordinate their priorities for resources.
 - c. Assess the impact that recommended OPSEC measures will have on their organisations and the operational effectiveness of friendly forces.
 - d. Assess the contribution of OPSEC measures to the wider C2W plan and, in particular, elements of the deception plan.
 - e. Ensure close co-operation with allies on all OPSEC measures.
 - f. Be involved in the identification of EEFI.

Specific Responsibilities

3. **Operations Staff (G3).** Responsibilities of the G3 staff include:
 - a. In conjunction with G2, identification of the EEFI of a particular operation/exercise.
 - b. The co-ordination of the OPSEC process and selection of the OPSEC measures within the unit or formation.

- c. The development and promulgation of the OPSEC policy and plan.
- d. Formulating any supporting deception plan.
- e. Co-ordinating the continuing evaluation of the execution of the OPSEC plan.
- f. Acting as a central point for monitoring and reporting OPSEC breaches.

4. ***Electronic Warfare Co-ordination Cell (EWCC)***. Responsibilities of the EWCC:

- a. In conjunction with G2 and specialist advisors, making an assessment of an enemy's (or his allies'), capability in ESM and ECM relative to the defined EEFI.
- b. An assessment of the vulnerability of friendly electronic systems to an enemy's ESM and ECM.
- c. The provision of advice to G3 Ops and formulation of plans to conduct ECM against the Enemy's ISTAR assets.
- d. The provision of advice to G3 and formulation of plans to conduct ECM against an enemy's ISTAR assets.
- e. Advising on Electronic Protection Measures (EPM).
- f. Assistance in monitoring and assessing the effectiveness of OPSEC measures.
- g. Assistance with deception planning.

5. ***Intelligence Staff (G2)***. Responsibilities of the G2 staff include:

- a. In conjunction with G3, identifying the EEFI.
- b. Assessment of an enemy's (or his allies'), ISTAR capabilities and ability to detect the defined EEFI.
- c. An assessment of friendly capabilities to counter enemy intelligence acquisition efforts.
- d. Advice on, and assistance in, the implementation of OPSEC measures.
- e. Advising on breaches of OPSEC revealed through analysis of enemy actions.
- f. Participation in deception planning, including the integration of OPSEC and deception.
- g. Liaison with, and where appropriate, direction of, specialist Intelligence and Security units.

6. ***Civil Military Co-operation (CIMIC) Staff (G5).*** Responsibilities of the G5 staff include:
 - a. Assistance in assessing the support of the local population for the enemy's aims.
 - b. Advice on, and assistance in, the implementation of OPSEC measures affecting the local population, eg movement controls.
 - c. Assistance in assessing the effectiveness of OPSEC measures as applied to the local population.
 - d. Liaison with Military Intelligence units.
7. ***Communications and Information Systems (CIS) Staff (G6).*** Responsibilities of the CIS staff include:
 - a. Advising on, and monitoring of, Force EPM, COMSEC, ELSEC and EMCON.
 - b. Advising operations and intelligence staffs of COMSEC, ELSEC and EMCON breaches.
 - c. Assistance and advice on deception planning.
8. ***Combat Service Support (CSS) Staff.*** Responsibilities of the CSS staff include:
 - a. An assessment of the vulnerability of CSS activity to enemy ISTAR activities.
 - b. Advice on the OPSEC measures to be implemented.
 - c. The implementation of OPSEC measures.
9. ***Other Staff.*** Other Special-to-Arm and Service advice will need to be sought. This will come from principal and special staff officers on the HQ staff. It may also be sought from specialist units supporting the force. The advice will be on details of the tasks in an operation, the potential indicators and vulnerabilities detected and proposed OPSEC measures to protect or control those indicators. The following provide specialist advice:
 - a. *Meteorological Services.* Weather, atmospheric conditions, visibility, prevalent cloud/mist cover.
 - b. *Engineers/Terrain Analysis.* Vegetation cover, intervisibility, dead ground, alternative routes.
 - c. *Media Operations.* Media activity and coverage.
 - d. *Provost Services* (directly or as liaison to local police). Closing roads/routes, out-of-bounds areas and curfews for friendly personnel and local population.

10. ***Military Intelligence (MI) Units.*** MI units will have an important role in OPSEC, particularly in rear areas and Operations Other Than War (OOTW). They will act as both force advisors on OPSEC measures and reaction forces where necessary. They will play an important role in security intelligence operations, in a liaison function, and in monitoring certain aspects of the OPSEC plan.

SECTION 2 - INTELLIGENCE REQUIREMENTS OF OPSEC

11. The basis of effective OPSEC is a good knowledge of the enemy's ISTAR systems. Intelligence support for OPSEC planning, therefore focuses on the capabilities and limitations of the enemy's ISTAR systems, including his decision cycle and any bias towards certain information/intelligence collectors or disciplines.
12. Counter-intelligence resources will be concentrated on the security threat. HUMINT, SIGINT and IMINT are important to assess the effectiveness of the OPSEC plan. Key information/intelligence requirements to support OPSEC are:
 - a. Capabilities of the enemy's ISTAR assets, including those of sympathetic nations/organisations.
 - b. Capabilities of enemy to process and analyse information and intelligence.
 - c. Intelligence on the enemy's intelligence objectives and achievements.
 - d. Factors, eg cultural bias and expectations that could influence the enemy's interpretation of intelligence gained.
 - e. Assessment of enemy's ISTAR and counter C2-capabilities to allow OPSEC planners to prioritise targeting and protection measures.
 - f. Counter-intelligence on the security threat posed by agents of foreign intelligence services (FIS) and sympathetic organisations.
 - g. HUMINT, SIGINT and IMINT on the effectiveness of OPSEC.

PART C

DECEPTION

CHAPTER 1

BACKGROUND TO DECEPTION

SECTION 1 - THE OPERATIONAL ENVIRONMENT

1. Deception is defined as: those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests¹.
2. Future battles are likely to be fought by comparatively smaller, but more mobile and lethal forces than in the past. Operations, invariably joint and mainly combined or multinational, will be conducted at high tempo, simultaneously in and from the air, in and with the electromagnetic spectrum, on and from the sea and on land in deep, close and rear engagements. The battlespace will almost certainly be non-linear, with greater opportunities for both sides to conduct bold manoeuvre and achieve surprise at all levels. Such a battlespace will put a premium on deception, both to achieve surprise and to disguise or conceal vulnerable or open sectors. A primary consideration for commanders will be the need to get inside the enemy's decision/action cycle - successful deception goes further in that it allows the Commander to control a major part of the enemy's decision-making process.
3. UK doctrine conforms to the manoeuvrist approach to operations², in which shattering the enemy's overall cohesion and will to fight is paramount. The emphasis is on the defeat and disruption of the enemy - by taking the initiative, and applying constant and unacceptable pressure at the times and places the enemy least expects. Deception is a natural corollary to this approach as it seeks to lead the enemy to expect, and thus prepare to meet, one particular friendly course of action, whilst actually striking elsewhere, or in a different manner or timescale.
4. The British emerged from the Second World War with an unequalled reputation for expertise in tactical and strategic deception. Since then, many of the skills have been forgotten and few have been taught and practised in any consistent fashion, although tactical deception has played its part in many OOTW situations. As General Eisenhower said in 1947:

"No major operations should be undertaken without planning and executing appropriate deceptive measures. As time goes on...there is the danger that these two means may in the future not be considered adequately in our planning. I consider it essential that the War Department should continue to take those steps that are necessary to keep alive the arts of...cover and deception."

5. Recent neglect of deception as a battle factor can in part be attributed to the view that advances in technology are progressively making deception more difficult, if not

1. AAP-6.

2. British Defence Doctrine, JWP 0-01.

impossible, to achieve. The increasing sophistication and proliferation of modern ISTAR systems has, to some extent, rendered the battlespace transparent, making deception harder to achieve. Such systems can be deceived but the effort required to make the deception credible may be considerable and beyond the scope of the forces in theatre. Fortunately these systems are still not widely available but where they are deployed, and there is a need to counter their capabilities, they can still be degraded, neutralised or destroyed by offensive action. The human mind, which is the target of deception, has not changed and remains as susceptible as ever to being deceived.

6. Deception is not just a tool of general war. It was used extensively at unit and formation level by both sides in the Vietnam War, and against the Soviet forces in Afghanistan.

SECTION 2 - THE PURPOSE OF DECEPTION

7. The purpose of deception is to mislead the enemy and thus persuade him to adopt a course of action (which may include continuing on his existing course, or doing nothing at all) that is to his disadvantage and which can be exploited. Where possible, this is achieved by reinforcing existing preconceptions or perceptions. Deception is a force multiplier and the employment of a relatively small proportion of a force on deception-related tasks can achieve benefits out of all proportion to the numbers involved. Deception is not an intellectual battle of wits for its own sake, neither is it a device merely to confuse the enemy - the object of deception is to convince the enemy to take a specific action. It follows, then, that any deception plan must be derived from, and be directly supportive of, the Commander's mission. At the same time, deception also aims to achieve:
 - a. *Surprise.* A successful deception plan will disguise or conceal friendly intentions, strengths, vulnerabilities and dispositions.
 - b. *Security.* Deception aims to portray a false friendly course of action. The enemy should believe that he has located and identified major elements of the friendly forces, their intentions and capabilities; thus providing security for the real forces, dispositions and movements. Security should be further enhanced by the OPSEC plan integral to the deception plan.
 - c. *Freedom of Action.* By occupying enemy forces in meeting a supposed threat, the Commander achieves greater freedom of action elsewhere on the battlefield. Deception is a key tenet of the manoeuvrist approach, and is particularly relevant to shaping and protecting the battlefield as well as in attacking operations.
 - d. *Economy of Effort.* Deception can reduce expenditure of time and resources, and save lives of friendly troops.

SECTION 3 - PRINCIPLES OF DECEPTION

Levels

8. **Strategic.** Strategic deception is designed to mislead the enemy as to the intent, time, place, strength and nature of intended operations at the highest level. By its nature, strategic deception is usually long-term and may need to be sustained over a period of months, involving a number of organisations, including National Agencies, in its planning and implementation. It is normally planned at national or theatre level by as small a team of specialists as possible, working direct to a Commander-in-Chief or appropriate government minister.
9. **Operational.** Operational deception covers in-theatre plans to mislead the enemy about the conduct of operations by formations. It may complement a strategic deception plan. At the operational level, deception is normally short-term in support of a particular phase of an operation.
10. **Tactical.** Tactical deception incorporates all measures to mislead the enemy on the battlefield which are planned at brigade level and below. Tactical deception may also be used to complement an operational deception plan. At this level, deception will be short-term and will concentrate on camouflage and concealment.

Principles

11. **Clear Aim.** Deception has to have a clearly defined aim which specifies the desired end-state and supports the real operational plan.
12. **Centralised Control and Staff Co-ordination.** Success in deception depends on a high degree of co-ordination and co-operation between staff branches in the planning, execution and monitoring of the plan. This will be facilitated by implementing deception as part of an overall C2W¹ plan. Deception schemes lacking co-ordination can cause dangerous confusion amongst friendly forces and can compromise the deception plan itself by revealing to the enemy obvious disparities in activity between neighbouring forces. Deception has to be co-ordinated and controlled at the highest level of command involved in the operation.
13. **Preparation.** Deception needs to be directed at a specific human target, which is normally the enemy commander at a given level, and be based, if possible, on his biases and likely reactions. All the measures needed to support and monitor the deception scheme should be thoroughly prepared, together with calculation of the target's reaction to each phase. Resources have to be allocated to tasks.
14. **Accurate Intelligence.** Deception has to be founded on accurate and timely intelligence about the enemy's doctrine, Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) capability, the enemy commander and his decision-making processes, the enemy's intentions and his knowledge of friendly intentions. Friendly ISTAR should have the capability to monitor and evaluate the effectiveness of the deception as it progresses.

1. See Part B Chapter 1 Paragraph 4

15. **Timing.** The timing of a deception plan is crucial. The enemy must be given sufficient time to notice, interpret and react to false information, but insufficient time to analyse it so thoroughly that the deception becomes apparent. Deception plans should be timed to create maximum disadvantage for the enemy at the decisive moment of real operations.
16. **Credibility.** Deception should never seem incongruous or illogical and must, where possible, accord with a pattern of events the enemy has reason to expect. When this is not possible, false information has to be supplied to him indirectly and in such a way that the enemy can work out the implications for himself. Conclusions derived from false information by deductive analysis carry more conviction if regarded by an enemy intelligence analyst as the result of his own astuteness.
17. **Corroboration.** False indicators have to be presented to the enemy through as many means as possible. Confirmation from these multiple sources should not produce too gratuitous or complete a picture as to arouse suspicion, but be sufficiently persuasive for him to take the bait.
18. **Security.** Although deception entails the intentional release of information to the enemy, security is still paramount. It is necessary to restrict access to plans, to brief friendly forces on a “need to know” basis and, at formation level, to implement the OPSEC process. Who needs to know what about deception is often a matter of fine judgement but it may be necessary, for example, to conceal from troops taking part in a diversionary attack the true purpose of their operations. Security of real plans is essential to deception and whenever indications of genuine activity cannot be wholly concealed they should be discredited by inferring that they are part of an obvious deception plan.
19. **Flexibility.** Flexibility is essential in order to take advantage of the enemy’s reactions, both predicted and unforeseen. In the event of the deception’s failure or only partial success, flexibility is also required to abandon or change the deception plan without revealing its original aim. To ensure this flexibility, and exploit enemy developments, deception plans should be continuously monitored by the controlling staff.

CHAPTER 2

THE DECEPTION TARGET

SECTION 1 - THE ENEMY

Enemy Organization

1. **National Characteristics and Historical Background.** Most nations exhibit distinctive characteristics which result from their history, geography, ethnic and religious make-up, political and leadership system, economy, class structure and a myriad of other factors which have shaped their destiny. These characteristics will have influenced, and have been influenced by, their armed forces. These in turn will have their prevailing characteristics and sensitivities which will influence the way they perceive the actions of others, and thus will indicate their susceptibility to deception (or to certain techniques) and may provide suitable avenues for exploitation.
2. **The Commander.** The deception target is the mind of the enemy commander whose decisions will lead to the fulfilment of the deception aim. Targets therefore appear at every level from heads of government at strategic level to formation, unit, and sub-unit commanders at the tactical level.
3. **The Command Structure.** The deception target, ie the commander, does not work alone. A detailed knowledge of the enemy command structure and process is required: command personalities and their decision-making processes; national political and military structures; and doctrine. At the higher command levels, much of this information will be available from the Defence Intelligence Staff, who may have biographical details of key enemy commanders. An approach that would deceive a bold, intuitive commander might fail against a more pedestrian, methodical leader, and *vice versa*. The influence or effectiveness of the enemy commander's staffs, particularly his intelligence organisation, is important. Different commanders attach different importance to their staffs:

"Deception operations against the Japanese in WW2 were largely ineffective. The Deception authorities were able to persuade Japanese intelligence "to swallow the most outrageous and implausible fabrications", but the operational staffs ignored them. It became clear at an early stage that the Japanese military held its intelligence services in low esteem and attached limited value to any information emanating from that quarter"¹.

A study of an enemy's military doctrine will also reveal much about his command structure and procedures.

4. **National Leadership Style.** The influence of national leaders and the system of government on their military commanders may be important; for instance, in WW2

1. British Intelligence in the Second World War, Vol 5 - Strategic Deception.

Hitler imposed his ideas on his generals and constrained their actions to a far greater extent than did Churchill. This could be significant in selecting the deception target - when planning a deception against the forces of a regime governed by a dictatorial leader who maintains a very close overwatch on his military forces, it may be necessary to target deception at the strategic level in order to influence the operational commander.

The Enemy's Thinking Processes

5. All targets have a number of vulnerabilities in common and these stem from the characteristics of the human mind. Psychologists have identified several tendencies which make the mind particularly susceptible to deception:
 - a. *Preconceived Ideas.* The brain accumulates a database of hypotheses. These are developed gradually with experience, a process otherwise known as learning. The process of thinking amounts to testing the current situation against the accumulated hypotheses in the mind. If the situation, as it is perceived, fits the hypotheses, the mind is liable to accept and believe it. The mind therefore relies upon preconceived ideas.
 - b. *Wishful Thinking.* The mind is gratified by evidence, which confirms its preconceptions. It can therefore attach undue importance to evidence that tends to support its theories and can reject evidence which fails to support them. Human nature reinforces this tendency by the common practice of subordinates telling their leaders only what they like to hear².
 - c. *Clarifying Uncertainty.* The mind finds coping with ambiguous situations very stressful and makes every effort to crystallise and clarify uncertainty. The temptation to jump to conclusions is all the greater under the pressure and stress of battle.
 - d. *Filtering Information.* The mind receives information from a number of sources. However, it filters the information it receives and the subconscious allocates its own priorities. It focuses particularly on anything new or interesting; this can be used by the deceiver to direct the target in the desired direction.
 - e. *Finite Capacity.* The human mind has a finite capacity for processing information. The large amount of information reaching an enemy may exceed this capacity, which in turn leads to his focusing on information supporting his preconceptions whilst ignoring evidence of other activity.
 - f. *Regularity.* The mind can be hypnotised by regularity. It pays less attention to events which occur over and over again and is bad at spotting small or gradual changes.

2. "The temptation to tell a chief in a great position the things he most likes to hear is the commonest explanation of mistaken action" Winston Churchill, *The World Crisis*, 1923.

The Enemy ISTAR Capability

6. The route to the target is through his eyes and ears, ie the enemy's ISTAR. If deception is to work, therefore, the enemy has to be supplied, via his ISTAR assets, with a flow of indicators to allow him to build up the desired picture of friendly activities. It has to be assumed that during the pre-conflict phase an enemy will have built up a database on friendly forces through espionage, IMINT, SIGINT, open source material and possibly monitoring of exercises. An essential part of the G2 staff's duties prior to the commencement of operations is therefore an assessment of an enemy's ISTAR capability, and the extent of his knowledge of friendly forces' capabilities, intentions, operational art and tactics. These can be exploited for deception purposes in conflict. Once conflict has commenced, the G2 staff is responsible for updating this assessment in the light of developments so that deception plans are not compromised by intelligence already in the enemy's possession. At the same time, the G2 staff should attempt to identify enemy preconceptions or expectations for subsequent exploitation.
7. Although the quantity, capability and variety of potential enemy ISTAR assets are daunting, there are practical limitations which can be exploited for deception purposes:
 - a. Sensors will detect and report only what they are designed to detect and report. They cannot discriminate or form a judgement.
 - b. Sensors and the associated C³I systems can be neutralised by active and passive countersurveillance.
 - c. Some systems do not have an all-weather capability.
 - d. Many systems cannot cover dead ground.
 - e. Many systems can be saturated by decoys and other means.
 - f. Information may not immediately available to the commanders who might use it.
 - g. The intelligence staff are liable to 'data saturation'; they may be inundated with large volumes of data and, lacking the capacity to process it all within the required timeframe, may be tempted to concentrate on information considered more reliable or plausible or data which is easy to evaluate.
8. No enemy has an all-embracing ISTAR capability. His ISTAR effort will therefore be directed in accordance with his perceived priorities, which will inevitably limit the coverage and search area of some sources. The priority attached to targets will change according to the stage of an operation. These targets, and their priority, will vary according to the enemy, his ISTAR capability, perception of friendly operations, concept of operations and doctrine. However, the following are likely to be priority ISTAR targets in most operations:

- a. HQs and other C2 facilities, and communications nodes.
- b. Precision weapons, helicopter forward operating bases and MRLs.
- c. Air defence assets.
- d. Other artillery and mortars.
- e. Major friendly groupings.
- f. Obstacles, natural and emplaced.
- g. Mobility corridors.
- h. Theatre point of entry.

SECTION 2 - THE IMPLICATIONS FOR DECEPTION

9. Several deductions may be drawn from this cursory study of the sources available to the modern target. These are:
 - a. Before deception measures can be planned, friendly ISTAR effort has to be directed towards establishing the type and density of the enemy's sources and towards looking for weak spots.
 - b. The greater the quantity and overlap of the target's sources, the more difficult is the deception task. The deceiver should therefore select those sources which are most easily fooled, whilst neutralising the remainder by active OPSEC and countersurveillance.
 - c. Deception plans should take advantage of weather and ground.
 - d. Deception measures should take advantage of the target's vulnerability to data saturation.
 - e. The reaction time of the target's sources has to be calculated and the timing of the deception plan established accordingly.
 - f. The deception plan and the active countersurveillance plan need to be co-ordinated, with the latter in support of the deception plan.
 - g. The deceiver has to dominate the enemy's use of the electromagnetic spectrum so that false information can be conveyed and genuine information denied. The deceiver should also control use of the electromagnetic spectrum by friendly forces. Substantial effort is required to guarantee this, though a lesser effort may still succeed in shifting the balance of probability in the target's mind.

CHAPTER 3

DECEPTION TECHNIQUES

SECTION 1 - THE APPROACH

General Points

1. Deception cannot be taught as a drill or SOP; there is no general-purpose deception plan. Such an approach would be self-defeating since deception relies for its success upon a large measure of originality and the unexpected. Furthermore, deception plans have to be tailored to the specific circumstances which prevail at the time. This Chapter examines broad techniques and methods of conveying information to an enemy, which can be used as a basis for a bespoke deception plan. It is comprehensive but by no means definitive.
2. The primary aim of deception is always to mislead the enemy and thus persuade him to adopt a course of action (COA) that is disadvantageous to him. The techniques and activities described in this chapter can be used, singly or in combination, to mislead the enemy, by disguising or giving a false picture of one or more of the following:
 - a. *What* is going to happen? What are friendly intentions: attack; defence; advance, withdrawal; move or do nothing?
 - b. *Why* are we doing it? What are our intentions and objectives, short and longer term?
 - c. *Who* is going to do it? Which units or formations are involved? Are they strong, weak, armoured or dismounted?
 - d. *Where* are we going to do it? Where will an operation happen; centre; flanks; rear; along a valley or across a river?
 - e. *When* are we going to do it? When will an operation happen: immediately, in hours, days or weeks; or perhaps never, if we wish the enemy to think it has been aborted?
 - f. *How* are we going to do it? What methods and tactics are we going to use: frontal attack; infiltration; encirclement; take a strongpoint or bypass it?

Deception Activities

3. There are a number of deception techniques and activities that can be used in a deception plan. Ultimately, however, deception consists of two complimentary activities:
 - a. *Simulation*. Simulation involves showing the false; allowing the enemy to see activity, equipments and positions. How this is done will depend upon the nature

of the deception plan. For a simulation to appear believable the enemy must be presented with the picture he has reason to expect. A professional army, such as the British, would be expected to show a high standard of camouflage and concealment drills. Simulation activity, therefore, should appear to the enemy to be the result of hasty or slightly imperfect camouflage - not a blatant display.

- b. *Dissimulation.* Dissimulation involves hiding the real; concealing it completely or making it appear to be something else. Dissimulation, in conjunction with OPSEC, is vital to concealing the underlying real activities behind the deception.

SECTION 2 - DECEPTION TECHNIQUES

- 4. There are a number of deception techniques, variations or combinations of which form the basis of all deception plans:
 - a. *The Obvious Solution.* Reinforcing the impression that an obvious way of achieving the objective has been adopted, whilst actually taking a different COA.
 - b. *The False Routine.* Conditioning the enemy by repetition to believe that an apparently standard routine will be pursued whilst in fact preparing a quite different course of action.
 - c. *Substitution.* Leading the enemy to believe that nothing has changed by covertly substituting the false for the real - and vice versa.
 - d. *The Lure.* Presenting the enemy with what appears to him to be a sudden or ideal opportunity which he must exploit, whereas he is in fact being lured into a trap.
 - e. *The Mistake.* Leading the enemy to believe that valuable information has come into his possession by mistake, through a breach of security, negligence or inefficiency.
 - f. *The Piece of Bad Luck.* Convincing the enemy that he has acquired information of vital importance by accident, because of a train of circumstances over which his adversary had no control.
 - g. *The Deliberate Leak.* The deliberate dissemination of information via agents or other clandestine links in such a way that the enemy believes he has obtained a piece of vital intelligence through skilful intelligence work.
 - h. *Exploit Enemy C2.* Several nations use automated processing systems as part of the C2. If their characteristics are known, these can be exploited to support deception, eg by information overload. Similarly, over-reliance by an enemy on a trusted source such as EW¹ or espionage can be exploited.

1. The Japanese relied almost entirely on SIGINT for intelligence at the operational level and above in WW2.

SECTION 3 - TYPES OF DECEPTION ACTIVITY

5. **General.** No deception plan will work when based on a single piece of information. The latter three techniques in paragraph 4 in particular will need to be corroborated by other sources. Deception can be broken down into the six basic activities below, a combination of which can be used to help build up the desired impression in order to deliver a complete picture, with corroborating information, to the enemy.
6. **Countersurveillance.** Countersurveillance (see Part A) covers all 'hiding and disguising', normally by camouflage, concealment, track discipline, absence of movement, radio silence and other passive measures taken to conceal the presence of a unit, formation or installation. It also covers active measures, such as increased air defence to prevent aerial reconnaissance and increased patrolling to deter ground reconnaissance patrols. Basic countersurveillance drills should be part of SOPs; the OPSEC plan accompanying any deception plan will include force-wide countersurveillance measures.
7. **Display.** A display is any means used to attract the enemy's attention and has the effect of confusing and misleading him as to the nature, size, intentions and exact location of the force opposing him. Thus it includes all decoys, mock-ups, dummy positions, equipment and obstacles, simulated tracks, heat sources, radio traffic, radar reflectors ("corner" reflectors) and other means of portraying a unit that does not exist, or giving the impression of large forces in an area where there are very few troops, or will disguise the true nature and strength of a unit or formation that cannot be concealed. A false ORBAT can be created, with additional units and formations. This technique was used extensively during WW2, but success is most likely in general war, with its accompanying mobilisation and activation of new units; or in expeditionary operations where the enemy is uncertain of the size and composition of the expeditionary force.
8. **Feints.** A feint is any movement made with the object of deceiving an enemy as to a commander's real plans. The purpose of a feint is to distract the action of an enemy force by seeking combat with it. Feint operations include attacks designed to mislead the enemy as to the direction and weight of a main thrust, feigned withdrawals to lure the enemy into a trap, diversionary raids and the like. They also have the object of persuading the enemy to redeploy his force, alter his supporting fire plan, deploy his reserves in the wrong place at the wrong time, or reveal a carefully concealed position by firing prematurely.
9. **Demonstration.** A demonstration is an attack or show of force on a front where a decision is not sought, made with the object of deceiving the enemy. The purpose of a demonstration is to distract the enemy's attention, without seeking contact. However, the possibility of the enemy responding by attacking the demonstration force should not be discounted.
10. **Ruse.** A ruse is any trick, stratagem or artifice designed to deceive the enemy.

11. **Electronic Deception (ED).** Electronic deception is radiation, alteration, absorption or reflection of electro-magnetic (EM) energy in a manner intended to confuse, distract or seduce an enemy or his electronic systems². Whilst deception based solely on ED is unlikely to succeed, ED is an essential part of almost any deception plan. The Electronic Warfare Co-ordination Cell (EWCC) at formation level is responsible to G3 for all aspects of ED within the overall deception plan, and will provide information on the enemy use of the electro-magnetic spectrum (EMS), vulnerability, ESM capabilities and the enemy's likely reaction to the ED element of a deception plan. ED is particularly effective when the enemy is: heavily reliant on the EMS for surveillance; dependent on the intercept of friendly EM emissions; when it is fully integrated into the overall operation; and when it provides one co-ordinated element of a multi-spectral deception plan. ED, through past experience, has included simulation of own nets, manipulation of traffic flow in order to give the wrong impression of intent, and imitation of enemy traffic. ED assets will require the capability to introduce false traffic (electronic and voice) onto enemy communications and the capability to record and subsequently retransmit message traffic if it is to make an effective contribution to deception. ED may be considered under three headings:
- a. *Manipulation.* Manipulation is the alteration of a force's electronic characteristics to counter enemy ESM activities. The object of manipulation is to fool the enemy into accepting the electronic characteristics presented as the real thing, leading him to an incorrect assessment of ORBATs, capabilities and intentions. Manipulation techniques include:
 - (1) False traffic levels.
 - (2) False or controlled routing.
 - (3) Traffic flow security.
 - (4) Controlled breaches of security ("leaks").
 - (5) Passage of formatted messages linked to certain operations or phases of war.
 - b. *Simulation.* Simulation within ED is the electronic representation of units and formations. It can be used to portray false locations, deployments, ORBATs and capabilities. Simulation techniques include:
 - (1) *False locations.* The electronic signature of a unit or formation is transmitted from a false location, while the real unit or formation maintains radio silence and communicates by other means.
 - (2) *Changed Equipment ORBAT.* The electronic signature of either new or different equipment is transmitted from within a unit, to mislead the enemy into believing that it has an enhanced or reduced capability.

2. ATP 51(A) - EW in the Land Battle.

- c. *Imitation.* Imitation is the injection of false and misleading information directly into the enemy's communication systems. The "imitator" must gain admission to the system as a "bona fide" user, and maintain this until the required information has been passed to the enemy. The electronic manipulation of recordings offers opportunities for imitation. Techniques include:
 - (1) *Nuisance Intrusion.* Voice broadcasts on a net designed to annoy or distract the operator.
 - (2) *Planned Message Intrusion.* Giving false information or orders to the enemy to delay or misdirect him.
 - (3) *Cryptographic Intrusion.* Disruption of cryptographic systems.
 - (4) *Deception Jamming.* The distortion of active electronic sensor returns, for example the use of corner reflectors to reduce the effectiveness of airborne surveillance radars. Normally a non-communications technique.
12. **Examples.** Annex A gives examples of battlefield deception and supporting measures which can be used to build up the desired picture.

EXAMPLES OF BATTLEFIELD DECEPTION AND SUPPORTING MEASURES

Ser	Method and Objectives	Examples	Control	Comments
(a)	(b)	(c)	(d)	(e)
1	Diversion To divert the attention and forces of an enemy from the point of the principal operation.	a. Diversionary Attack.	Fmn, Unit	Depletes resources available for the principal operation but a 'scratch' force may be used.
		b. Diversionary Bombardment.	Fmn	Potential benefits have to be weighed against availability of guns and ammunition.
		c. Diversionary Air Attack.	JFHQ	Potential benefits have to be weighed against availability of sorties.
		d. Diversionary Assault in depth.	JFHQ	1. Suppression of air defences. 2. Aircraft or helicopter lift. 3. Subsequent logistic support.
		e. Diversionary illumination or smoke.	Fmn, Unit	1. Short term measure. 2. Availability of illumination/smoke. 3. Normally accompanied by offensive measures.
		f. Diversionary noise.	Fmn, Unit	1. Problems of amplification. 2. Normally accompanied by some offensive measures.
2.	Decoy a. To lure the enemy into a trap. b. To lure the enemy away from a particular area or route. c. To proliferate targets. d. To support a diversion.	a. Establish an obvious routine and encourage the enemy to exploit it.	Fmn, Unit	Ambush approaches to a routine VCP in OOTW, for example.
		b. Drop marked maps showing false information.	Fmn	Likely to arouse suspicion and must therefore be supported by other measures.
		c. Controlled breach of security.	JFHQ	1. No guarantee that the enemy will intercept it. 2. One isolated breach may arouse suspicion. 3. Might be useful to support other measures.
		d. Decoy noise.	Fmn, Unit	1. May be used to draw indication of genuine activity. 2. Problems of amplification.
		e. When own position known to be compromised, ambush en forces sent to attack it.	Unit	More applicable to OOTW.

Ser	Method and Objectives	Examples	Control	Comments
(a)	(b)	(c)	(d)	(e)
		f. Decoy key equipments.	Fmn	See comments on dummies.
		g. Decoy signs and markers.	Fmn	Confusion of own forces has to be avoided.
		h. False fronts.	Fmn, Unit	1. Used to lure the enemy into expending resources before the decisive engagement. 2. Requires extensive deception effort.
		i. Dummy and alternative positions.	Fmn, Units	Can sometimes involve extensive time and resources.
		j. Decoy heat and light sources.	Fmn	1. Required either to support the credibility of decoy position or to lure missiles away from targets. 2. Heat sources must be realistic to fool TI, although heat-screening materials can "blur" the picture.
		k. Decoy optics	Unit	Simple simulations of key weapon systems to draw enemy fire.
3.	Demonstration a. To produce a show of force in an area where a decision is not sought. b. To misdirect or dissipate enemy forces. c. To enhance survivability. d. To create a false routine. e. To support a diversion or lure.	a. False movement of ground forces.	Fmn	Presupposes that only that part of the movement designed to deceive can be monitored.
		b. False air movements.	JFHQ	Empty troop lift helicopters, for example.
		c. False concentratinos.	Fmn	False concentrations can be created by real or dummy forces or a mixture or both but are expensive in time and resource.s
		d. Maintaining false electromagnetic signature and moving on electronic silence.	JFHQ	1. Planned and co-ordinated by EWCC. 2. Involves some radios and operators remaining whilst main force moves. 3. Maintenance of normal communications traffic needs practice. 4. Real movement has to be concealed, particularly from standoff radar. 5. As an alternative, the reverse may be practised, ie moving formations or units electronically whilst the real force remains static.
		e. Manipulating the level of radio traffic to signify false impending activity or inactivity.	JFHQ	1. Planned and co-ordinated by EWCC. 2. Assumes that the enemy will intercept and interpret correctly. 3. Must be supported by other measures
		f. Running false radio nets, eg traffic control net.	JFHQ	1. Planned and co-ordinated by EWCC. 2. Assumes that the enemy will intercept. 3. Additional radio resources required. 4. Use of the relevant already over-crowded bands of the electromagnetic spectrum will require co-ordination.

Ser	Method and Objectives	Examples	Control	Comments
(a)	(b)	(c)	(d)	(e)
4	Dummy a. To support a decoy. b. To support a demonstration.	a. Dummy defensive positions.	Fmn, Unit	1. Consumes time, manpower and defence stores. 2. Needs plausible electromagnetic signature. 3. Needs a proportion of real forces if the deception is to be sustained.
		b. Dummy HQ and Commcens.	JFHQ	1. Expensive to sustain the necessary electromagnetic signature for long. 2. Needs to be supported by physical indicators like heat sources, antennae, signs.
		c. Dummy key equipments and signature equipments.	JFHQ, Fmn	1. Expensive in manpower and resources. 2. It may be more cost effective to disguise real key and signature equipments.
		d. Dummy signs, insignia, helicopter marker panels.	Fmn	Danger of self-confusion has to be overcome.
		e. Dummy air defence systems with dummy or live radars.	JFHQ	1. Air defence systems are a high priority for enemy surveillance. 2. Completely dummy equipments have limited or local decoy value. 3. Use of live radars is more effective but expensive in manpower, equipment and use of the frequency spectrum. Where, however, sites for air defence radars are limited, exposure of this ploy can help the enemy deduce the location of real radars. 4. Pyrotechnics can simulate launch of additional missiles.
		f. Dummy minefields and other obstacles.	JFHQ	1. Dummy minefield and obstacles call for almost as much time and effort as real ones. 2. For best effect they also need to be covered by fire. 3. False rows may be profitably used to thicken up real minefields, plausibility being reinforced by false tilt rods and fuses.
		g. Use of civilian vehicles to provide heat and light sources.	Fmn, Unit	Cars, agricultural machinery.
		h. Use of damaged and unserviceable equipment.	Fmn, Unit	1. More realistic than inflatable or improvised versions. 2. Should be emplaced so damage is not apparent.
		i. Use of training stocks eg empty ammunition boxes.	Fmn, Unit	Decoy dumps and logistic installations.
		j. Dust raisers.	Fmn, Unit	Branches towed behind vehicles.

Ser	Method and Objectives	Examples	Control	Comments
(a)	(b)	(c)	(d)	(e)
		k. Noise.	Fmn, Unit	1. Vehicle or generator noise. 2. Charges to decoy enemy sound ranging equipment. 3. An assessment of the effectiveness of false noise against the background of real battlefield noise is required.
		l. Dummy artillery positions, firing and flash simulators.	Fmn	1. Pistol or roving guns are needed in the dummy position. 2. Firing and flash simulators have to be co-ordinated with the firing of live batteries. 3. Dummy batteries have to move.
		m. Corner reflectors to simulate vehicles and bridging.	Fmn	Effective against pulsed radar, but not synthetic aperture radar (SAR) or Moving Target Indicator (MTI) radars.
		n. Simulation of major damage to deter further attacks.	Fmn	1. Useful for fixed installations only. 2. Indications of subsequent use have to be concealed.
5.	Disguise/mimic/simulate a. To mislead the enemy by imitating his forces or his communications. b. To mislead the enemy by imitating civilians or civilian equipment. c. To enhance survivability.	a. Intrusion on enemy radio nets.	JFHQ	1. Planned and co-ordinated by EWCC as part of overall deception plan. 2. Difficult to achieve credibility without access to enemy equipment. 3. Expert linguistic ability and knowledge of enemy radio procedures required. 4. Taped voiceprints may be used but are useless if the target has the option of replying. 5. Can be immediately followed by jamming to prolong the effect.
		b. Use of captured enemy equipment and uniforms.	JFHQ	1. This trick has been used in the past to bounce reserved demolitions. 2. Prisoners, caught in disguise, may forfeit protection from the Geneva Convention.
		c. 'Q' vehicles.	Fmn	Requisitioned or abandoned civilian vehicles.
		d. Key equipments disguised as civilian vehicles or deployed inside container lorries.	Fmn	
		e. Swap radars between formations.	JFHQ	1. To prevent identification of formation boundaries from individually finger printed radars. 2. Previously unused radars may also be used.
		f. Use of LO vehicles to simulate unit HQs.	JFHQ	1. May be used in conjunction with false fronts, dummy positions. 2. Reproducing plausible radio traffic requires training.
		g. Radar Repeaters.	JFHQ	Devices which produce a false Doppler effect

Ser	Method and Objectives	Examples	Control	Comments
(a)	(b)	(c)	(d)	(e)
6	Substitution a. To enhance survivability. b. To mislead enemy sources. c. To dissipate enemy effort. d. To support a diversion. e. To support a decoy.	a. Replace a compromised real position with a dummy one.	Fmn, Unit	1. Create, for example, an obvious dummy bridge using floating corner reflectors, before deploying a real bridge in the same place. 2. Some risk that the enemy will fail to identify the dummy as dummy.
		b. Replace an obvious dummy position with a real one.	Fmn, Unit	
7.	Controlled Release of Information To support a diversion, decoy or demonstration.	a. Controlled rumour amongst the civilian population.	JFHQ	
		b. Allowing false documents or newssheets to fall into enemy hands.	JFHQ	Can be particularly effective in OOTW.
		c. "Leaks" to known enemy agents or sympathisers.	JFHQ	Deception cannot be achieved without effective
8.	Countersurveillance To prevent hostile surveillance of a real force, area or place.	a. Concealment or camouflage of all genuine indicators sought by enemy ISTAR.	Fmn, Unit	countersurveillance.
		b. Use of dead ground and built up areas.	Fmn, Unit	Maps showing areas of radar screening are useful.
		c. Use of bad weather.	Fmn, Unit	Note that darkness now confers only minimal concealment.
		d. EPM.	Fmn, Unit	EWCC will advise in conjunction with G6.
		e. Heat screens and deliberate fires.	Fmn, Unit	1. Materials which suppress heat emissions and radar reflectivity are under development.
				2. Creation of deliberate decoy fires may be counter productive and conflict with the need to maintain fields of observation and fire.
		f. Smoke.	Fmn, Unit	1. Limited quantities of smoke.
		g. Toning 'up' or 'down' of fixed installations.	JFHQ	2. Multi-spectral smoke to counter TI currently not held, but due in service in future. Depot, storage sites, airfields.
		h. Destruction or neutralisation of enemy ISTAR assets.	Fmn, JFHQ	As part of active OPSEC and countersurveillance measures.

CHAPTER 4

THE DECEPTION PROCESS

SECTION 1 - GENERAL POINTS

General

1. Deception should be an integral part of all operations¹. The Commander must consider deception as part of his analysis, rather than arriving at a decision first, and only then considering how deception could support his operation. By adopting this approach, deception is fully integrated into his plan and the co-ordination of all real and deceptive activities is facilitated. The deception element of the operations plan can assist in:
 - a. Masking intentions and objectives.) Thus
 - b. Masking capabilities, thus increasing their surprise effect.) causing
 - c. Masking vulnerabilities.) the
 - d. Masking timings and locations of crucial phases of an operation.) enemy
 - e. Masking locations and deployments.) to
 - f. Forcing the enemy onto ground of our own choosing.) take
 - g. Forcing the premature deployment of enemy forces.) actions
 - h. Diverting enemy reconnaissance effort.) contrary
 - i. Diverting enemy fire from both artillery and air.) to his
 - j. Diverting the enemy EW effort to unproductive areas.) interest.
2. The command and staff decision-making process for deception mirrors that for the main operation.
3. Deception should be an integral part of the Full Estimate² or the Quick Estimate. Where possible, a separate Deception Estimate should be conducted to ensure consideration of all relevant factors, and to maintain the “need-to-know” principle. The Deception Estimate follows the same pattern of mission analysis, evaluation of

1. ADP Vol 2 *Command*.

2. AFM Vol 1 Pt 8 *Command and Staff Procedures*.

factors, consideration of COA and the decision. The end result, the deception COA, should then be integrated into the overall Commander's Decision. In the case of the Quick Estimate, the need for deception will probably be derived from Stage 1, Preliminaries, as high-level intelligence on enemy intentions and preconceptions is unlikely to be available at this level. A suggested shortened format of the Deception Estimate for use at battlegroup level is at Annex A.

4. Once the decision to incorporate deception as part of an operation has been taken, it must be followed through to its intended conclusion. A deception that has not been thoroughly planned, prepared and implemented will soon become apparent to the enemy. This will allow him to discern real intentions, or even to mount his own deception by apparently meeting friendly expectations. For deception to be believable, considerable resources may have to be committed, which is particularly important when the overall resources available to a commander may be limited. The commander must consider this when deciding on the scale or scope of his intended deception.

SECTION 2 - MISSION ANALYSIS

General

5. The Deception Estimate starts with Stage 1 of the Estimate process. Once a commander has established the tasks necessary to fulfil his mission, he can consider how deception will assist their implementation. As part of the mission analysis, he has to consider the possible effects of deception:
 - a. *Superior's Intent.* Deception has to be approved by, and co-ordinated with, the superior commander. This is essential to avoid actions by a superior or flanking formation/unit compromising the deception and, equally importantly, to avoid diverting the enemy effort in a direction that would be contrary to the superior commander's wider interests.
 - b. *Specified and Implied Tasks.* The deception and its intended result should not contradict the superior commander's specified and implied tasks necessary to achieve the mission, particularly the requirement to support the superior commander's Main Effort.
 - c. *Constraints.* Specific constraints may include those of time, space, resources and Rules of Engagement (ROE). All these may impact upon deception.

Commander's Direction

6. On completion of the deception mission analysis, the commander gives direction to the deception staff on completion of the Deception Estimate. The rest of this stage of the deception estimate then follows that for the Commander's Estimate, except that an initial warning order is not usually issued, in accordance with the "need to know" principle. The deception staff's first priority will be to identify the critical information requirements for deception. These are likely to include:

- a. Any identified enemy preconceptions or expectations.
- b. Timescale for the deception.
- c. Broad outline of enemy ISTAR capabilities.
- d. Availability of own forces, assets and materiel.
- e. Need to involve non-organic sources and agencies.

SECTION 3 - EVALUATION OF FACTORS

Enemy

7. **General.** Deception is founded on accurate and timely intelligence on the enemy. The intelligence requirements of deception are given in Annex B.
8. **National Characteristics and Historical Background.** Consider:
 - a. National characteristics and background, including: dictatorial/democratic, centralised/decentralised, secretive/open, suspicious/receptive, commanders selected on ability or loyalty to regime.
 - b. Profile of national leadership, and identification of biases and perceptions.
 - c. Historical assessment of the enemy's experience of deception in recent conflicts.
9. **Deception Target (Centre of Gravity).** The enemy's centre of gravity for the purposes of deception is the relevant commander and his staffs. This has to be evaluated in detail as personal characteristics and leadership style, experiences, decision-making processes, biases, preconceptions and expectations can be exploited as part of a deception plan.
10. **Enemy Current Knowledge.** The extent to which the enemy is already aware of friendly intentions and plans may be assessed from insights into his decision-making process (normally derived from Signals Intelligence [SIGINT] and Human Intelligence [HUMINT]) and his current deployments and ISTAR priorities (from all sources). Other factors include:
 - a. Known or suspected compromise of information (including marked maps) due to security and COMSEC breaches or losses in action.
 - b. Media reporting of friendly activities.
 - c. What he could reasonably deduce given his ISTAR capability and any information from (a) and (b) above.

11. **Preconceptions.** Does the enemy already believe that friendly forces have a set objective? Preconceptions can be deduced from intelligence (normally derived from SIGINT and HUMINT) and his current deployments; they may also be derived from a psychological analysis of the enemy commander. Wherever possible, preconceptions should be used as the basis for the deception, it being easier to maintain an existing belief than to attempt to change it. Similarly, a change of friendly course of action can be used as a deception ploy by portraying the original plan as still ongoing.
12. **Deployments.** If no preconceptions or expectations can be identified, suitable avenues for exploitation by deception may be identified from current intelligence on the enemy's ORBAT, deployment, dispositions and intentions.
13. **ISTAR Capability.** The deception plan will focus mainly on the enemy's ISTAR assets, as these are his eyes and ears. Can he detect the desired indicators and, just as importantly, the underlying real activity? The enemy's capability to process the information gained into intelligence, and the influence his intelligence organisation has on the operations staff, should also be considered.
14. **Enemy's Communications Infrastructure.** The deception plan will need to identify and analyse the enemy's communications infrastructure in order to select those nodes or networks which may be suitable for exploitation by Electronic Support Measures (ESM) or ED. ESM exploits enemy communications for intelligence purposes, to identify enemy preconceptions or plans, and as part of the monitoring process as the plan proceeds. ESM can provide crucial indicators of the success or failure of the overall deception plan, and could provide early indications as to the adversary's reaction to the deception. ESM provides critical input into the overall database and will directly influence the ED plan. Certain enemy communications links will be vital to the success of deception plan by allowing the passage of intelligence traffic. Information passed by, for example, enemy armoured recce, or brigades' reports to higher headquarters, may be essential to building up the desired picture of friendly activities. It follows that friendly forces should allow these nodes and nets, and those being exploited by ESM and ED, to continue functioning while they contribute to the deception.

Environment

15. **Ground.** The plan has to be consistent with the ground. For the plan to be credible, its aim and any friendly dispositions portrayed must be realistic and in accordance with doctrinal models. The ground will affect the nature of deception operations and their implementation in two ways:
 - a. **Terrain.** The nature of the terrain will dictate the complexity of the deception plan and its implementation. Open terrain will require "display" techniques (dummy installations and equipment), which may require more detailed simulation. Deception in undulating, wooded or urban terrain can make greater use of concealment, and simulated activity may only need basic mock-ups. These should be camouflaged properly but "carelessly" to avoid being too blatant.

- b. *Weather.* Deception can take advantage of poor visibility, by using it to conceal real activities at critical phases of an operation, or to allow the use of less detailed simulation, particularly if enemy ISTAR relies heavily on the visual spectrum. However, it may also prevent enemy ISTAR from detecting vital indicators. It should also be borne in mind that the weather can be unpredictable.
16. **Local Population.** The presence or otherwise of local population, and their sympathies, can be critical to the success of deception. The local population can be used as a medium for the passage of indicators and controlled rumours to the enemy, but they can also, deliberately or unwittingly, compromise simulated and concealed activities. The OPSEC plan should take account of these factors.
17. **Media.** The presence of media representatives in the Area of Operations (AO) also has serious implications for deception. The media must not be used for the passage of false indicators and rumours, nor can they be told untruths. They can, however, be given access to real activities within the deception plan. The OPSEC plan must specifically address the issue of the media in the AO.
18. **Friendly Forces.** The examination of friendly forces should identify their availability and capability to conduct deception. The following should be considered:
- a. *Air and Maritime Situation.* If the enemy's ISTAR includes an aerial capability, this will influence the deception plan. Conversely, it may be necessary to allow aircraft to penetrate friendly airspace as part of the plan; the same considerations apply to his maritime capability, particularly in littoral operations. Air and maritime activity will usually be required as part of the deception plan, and at the same time, activity which could compromise the plan must be de-conflicted. This will require co-ordination at the highest level.
 - b. *Ground Formations.* Considerable co-ordination will be necessary with flanking, forward or depth formations.
19. **Friendly Resources Required.** This will examine the resources required to implement the deception. Considerable resources, both material and manpower, may be required. Consideration should be given to:
- a. *ED.* For ED to be effective, significant communications assets will be required. A typical UK brigade HQ will feature as an outstation or control station on approximately 15 separate nets in the HF and VHF band. In addition they will have trunk access via radio relay and single channel radio access in the VHF and UHF bands. A similar capability will be required to simulate this net usage realistically.
 - b. *Materiel Resources.* "Display" techniques may require substantial amounts of materiel. The sophistication of simulated positions and deployments will vary according to the enemy ISTAR capability, but resources will vary from locally-improvised dummies through to sophisticated inflatable AFVs complete with internal heat sources to fool thermal imagers. Damaged and inoperable vehi-

cles, positioned so that the damage is not visible, can be used, alone or mixed in with dummies.

- c. **Manpower and Equipment.** There is frequently no substitute for the real thing. Typical real manpower, equipment and materiel requirements for a dummy company group, gun positions and unit CP are given in Annex C. Even a simple display, such as a dummy sub-unit position, will require manpower and equipment to dig trenches, erect dummy vehicles, etc. Implementing a deception plan will involve risks, not the least of which will be the diversion of staff and force effort. The Deception Estimate should examine these risks under a "Risk Assessment" section.

- 20. **Timescale.** How much time do friendly forces have to convey the required indicators to the enemy, and over what period must the deception be maintained?
- 21. **Consideration of Any Other Relevant Factors.** Relevant factors can include ROE, legal constraints, the media and civil/military relations.
- 22. **Possible Options.** At this stage the deception estimate should have identified a number of possible deception aims and examined their feasibility in outline, including the availability of resources.

SECTION 4 - CONSIDERATION OF COA

- 23. **General.** The next stage is to identify deception COA based upon the identified aims. The advantages and disadvantages of each COA in relation to the mission are considered in order to establish the resources required and the risks involved.
- 24. **Risk Assessment.** An assessment of the risks involved in each COA must be made. Factors to be considered include:
 - a. Risk of compromise of the deception:
 - (1) Adequacy of resources.
 - (2) Enemy ISTAR capability.
 - (3) Local population and media
 - (4) Capture of knowledgeable personnel (eg troops involved in constructing dummies, etc).
 - b. Risk to the mission if the deception is compromised or does not result in the enemy taking the intended action: does it expose friendly forces to unacceptable risks?
 - c. Do the benefits of the deception outweigh the resources allocated to it?

SECTION 5 - THE COMMANDER'S DECISION

25. The commander decides which deception COA to adopt. He may decide not to employ deception, but he should only do this after full consideration of the COAs and the Risk Assessment.

SECTION 6 - DECEPTION PLANNING

26. **General.** Having decided the deception COA, a detailed plan should then be formulated. The deception and operational plans should be formulated in concert; where possible real and simulated events should be integrated to develop the desired picture. It is important to visualise events from an enemy perspective - what indicators does he need in order to come to the desired conclusion - bearing in mind the enemy's doctrine, personalities, existing knowledge and expectations? The plan needs to start with the end state - a specific action (or inaction) by the enemy. This becomes the aim of the plan. The planning sequence below follows that for the Deception Estimate.
27. **Aim.** G3 staff defines the aim, which is derived from the Estimate. It is expressed as a short statement of the desired end state, such as: *to cause the enemy to withhold committal of his reserves until D+3; or to cause the enemy to deploy his anti-tank reserve to the area of Hill 357 by D-1.*
28. **Friendly Activity.** G3 staff, in conjunction with G2, identifies the friendly activity that would cause the enemy to react in the intended way. This is outlined in a short (no more than 5 - 6 lines) paragraph in the deception plan. The signatures, indicators and events that, if detected, would point to such activity occurring are then identified. Considerations as to the most "profitable" indicators and events to include in the plan include all those in the estimate process, particularly:
- a. The enemy commander, and staffs/individuals assessed to have influence on him.
 - b. The enemy's knowledge of current friendly activity and intentions.
 - c. Efficiency and reaction times of the enemy's ISTAR systems. This will also involve a thorough understanding of the enemy's C2 system.
 - d. The expected time needed by the enemy to complete his actions and arrive at the desired end state.
29. **Sequential Plan.** Having identified those events that need to be portrayed as part of the deception, a sequential plan, with a detailed list of necessary resources, can be made, and synchronised with the Operations plan. The deception plan will need extensive co-ordination as failure to implement a stage, or a deviation in timings, could compromise the operation or result in the enemy misinterpreting the indicators. The plan should include the desired enemy reaction to each event, for use in the monitoring process. An example of a deception planning worksheet is at Annex D.

30. **Integration with the OPSEC Plan.** OPSEC is an integral part of deception. Deception aims to portray a false picture but no deception plan can be all-embracing. Where possible, activities forming part of the real operation should be used to reinforce the deception, but some real activities will inevitably have signatures that have to be concealed; thus an effective OPSEC plan, fully co-ordinated with the deception plan, is vital. An OPSEC analysis of all friendly activities, deceptive and real, is essential. This analysis will identify those real activities that has to be hidden, and those which support the deception plan. These may need to be “displayed”, and the OPSEC plan must take this into account. The OPSEC analysis may reveal enemy ISTAR systems which cannot be deceived using available means, or that, despite the implementation of effective OPSEC, may compromise the underlying real activities. These have to be destroyed or neutralised at the critical moment. If this is not possible, the deception may not be feasible. Of particular concern to deception is the presence of the media, who are often equipped with extremely capable communications and pose a potential security threat to deception operations. The OPSEC plan should cover access by the media to locations and forces in detail, and the G3 Media Operations staff may have to impose severe movement restrictions on accredited journalists to deny them access to sensitive areas. Advice on restricting the movement of unaccredited journalists and other civilian staff should be sought from Legal and Provost staffs. The integrity of G3 Media Operations should not be compromised by the use of the media to help portray deception measures.
31. **Distribution of the Plan.** The outcome of the deception planning process is the deception plan, which should be distributed on a strict “need to know” basis as an Annex to the Operation Order. To reduce the risks of compromise, units and formations involved in the implementation of deception should only receive extracts covering their immediate part in the operation.

SECTION 7 - THE CONDUCT OF DECEPTION OPERATIONS

General

32. The conduct of a deception operation has to be carried out strictly to timetable as the events laid down will enable the enemy to gradually build up the desired picture, in the order in which he would expect to see a pattern of events unfold. Any failure to meet the timings laid down in the plan has to be reported immediately to the deception staff for corrective action as necessary. The deception staff need to oversee and co-ordinate implementation to ensure that each event or measure is implemented by the appropriate unit/formation in the correct sequence and at the right time.
33. Implementing the plan may involve obvious simulation, such as constructing dummy equipment and positions, or transmitting false communications and signals as part of ED. In such cases those involved should be briefed only on their immediate role. Conversely, actual military activities may be required, the purpose of which may not be apparent to those involved. The information to be released will then depend on whether the activity is plausible and needs no detailed brief except on the task in hand; or if it will be apparent to forces involved that their actions are unusual. Should this be the case, the minimum amount of detail on the deception plan should be

released, bearing in mind the particular risk of compromising the whole plan should those involved be captured.

Monitoring

34. The G2 staff will, as part of their routine activities, monitor an enemy's actions. They will pay particular attention to the expected indicators and reactions given as part of the plan, as signs that the enemy is responding to the deception in the manner intended. In the early stages of a deception operation the main response to the plan will be in the perception of developing events in the minds of the enemy's staffs and personnel. EW, SIGINT and HUMINT are the main methods for obtaining insights into the enemy's thoughts and opinions. It may be necessary to mount specific actions to take prisoners for interrogation for this purpose.
35. Actual changes to deployment will be monitored by all means and will provide confirmation (or otherwise) that the enemy is taking the desired actions. If no activities indicating this occur, EW, SIGINT and HUMINT may need to be tasked to identify the reasons. While the deception may well have implanted the desired impression in the enemy intelligence organisation, the commander may be unwilling or unable to react to it in the desired way. HUMINT may be the best and only means of confirming the success of deception operations in PSO, where a change of behaviour is sought through changing perceptions amongst the local populace. Deception staffs should always be aware of the possibility of counter-deception as the enemy himself implements a deception that matches friendly expectations.

Changes or Modifications to the Plan

36. **General.** The deception plan may be extremely complex and will involve extensive co-ordination between many separate elements of the force. It will be implemented over a period of days or even, in some cases, weeks. It will contain many interdependent events, with seemingly minor occurrences (and their subsequent implantation in the enemy's mind) many days previously giving credence to later, larger events. Any changes to the plan must therefore only be made after detailed consideration of all available intelligence derived from the monitoring process. It is also possible that later changes, unless very carefully implemented, could compromise earlier stages of the operation by revealing inconsistencies. However, there are circumstances under which modifications or complete changes may be considered:
 - a. *Enemy Suspicions or Intelligence Failures.* EW, SIGINT or HUMINT may reveal that the enemy has suspicions about the indicators fed to him, or may have missed some, leaving him with insufficient evidence to lead him to the desired conclusion. It may then be necessary to reduce the flow of indicators, or to supply him with more. The first course of action carries the risk that he may then miss the point, and the second of being too blatant. They should not be contemplated unless there is a reliable means of monitoring the enemy's decision making process.
 - b. *Enemy Misinterpretations.* The enemy may misinterpret the indicators or respond in a manner other than that intended. Should the enemy adopt an

unintended course of action, it may be easier to allow him to continue with it, providing it is still to his disadvantage. Only if his adopted course of action offers little or no advantage to friendly forces will the deception plan need to be changed; this change must be seamless or he may detect inconsistencies that could compromise the whole operation.

SECTION 8 - OTHER CONSIDERATIONS

37. ***Protection for Deception Parties.*** Some forms of the lure technique involve relatively small deception parties revealing their presence to the enemy and inviting their own destruction. This type of mission is unlikely to be undertaken with enthusiasm unless the deception party can be given some protection either by evading before their position is attacked or by ambushing the approaches to their position.
38. ***Avoiding Self-delusion.*** One of the inherent dangers of deception is the risk of deceiving or at least confusing friendly forces. To avoid this danger it is necessary to brief troops thoroughly but on a strict “need to know” basis. To avoid accidental confusion, for example troops unconnected with the deception plan being misled by false route signs, consideration should be given to colour coding true and false indicators, the colours being changed periodically to maintain security. Once a deception plan has achieved its aim deception stores should be removed.
39. ***Training.*** The need to practise deception techniques in training has long been recognised but all too often overlooked. There is no shortage of ideas about how deception might be implemented but there is a distinct lack of detailed evidence based on recent experiment. Two particular constraints need to be overcome. The first is the habit of so compressing training and exercises that insufficient time is available to execute deception plans. The second is a concern about compromising deception plans by practising them in peacetime. There is however such a variety of deception techniques and measures that a discernible pattern of procedures can be avoided. Unit level training, particularly in defensive deception, should be a matter of routine. It will help to counter enemy deception measures if relevant training exercises at all levels include an element of the “unexpected”, thus inculcating flexibility of mind in our commanders.

SECTION 9 - COMMAND AND CONTROL OF DECEPTION

The Commander’s Responsibilities

40. Deception has to be controlled at the highest level of command involved in the operation. This is essential to ensure that:
 - a. The plan directly supports the Commander’s mission.
 - b. The efforts of all relevant staff branches are co-ordinated. This is particularly relevant when staffs or units are unaware of the deception plan, or of their part in it. This may frequently be necessary as part of the “need to know” principle.

- c. Individual units or formations do not take actions which could unwittingly compromise the plan.
 - d. Assets required to support deception are allocated.
41. Deception is the commander's responsibility. It is a G3 staff function, but must be co-ordinated with G2 staff. As deception is integral to C2W it should, where possible, be planned, implemented and monitored by a dedicated C2W cell. If no formal C2W structure exists, then it has to be compiled and monitored by a separate deception cell formed from trained personnel drawn from appropriate specialist staffs/advisors.

Staff Responsibilities

42. **General Points.** Overall responsibility for deception rests firmly with the G3 staff. Other specific subsidiary responsibilities are devolved as follows:
- a. *G2 Staff.* Advice on, and detailed planning of, deception using the facilities of the All Source Cell.
 - b. *G4 Staff.* Logistic support of deception.
 - c. *Artillery Staff.*
 - (1) Co-ordination of indirect fire and offensive air support.
 - (2) Artillery deception measures.
 - c. *Engineer Staff.*
 - (1) Co-ordination of engineer assistance in battlefield deception measures.
 - (2) Engineer deception measures.
 - e. *Electronic Warfare Co-ordination Cell* (JFHQ, Corps and Division; Bdes may have EW LO). Planning and co-ordination of electronic deception measures and advice on EPM.
 - f. *G6 Staff.* Assist in planning and deployment of electronic deception measures.

SHORT FORMAT FOR THE DECEPTION ESTIMATE

At battlegroup level the full Deception Estimate described in Section 1 to this Chapter may be inappropriate or too time-consuming. This shortened form is adequate for a simple deception at this level.

Serial	Stage	Considerations
(a)	(b)	(c)
1.	Mission Analysis: a. Own mission. b. Higher Commander's and flanking unit's missions.	How will deception support my mission? What is its aim? For how long must it be kept up? Will my deception adversely affect them?
2.	Evaluation: a. Enemy. b. Environment. (1) Terrain - open or close? (2) Weather - good or bad visibility? (3) Local population - present or absent? (4) Media - present or absent?	Does he use stereotyped tactics or individual initiative? Which level commander is the deception aimed at? What does he already know about my intentions? What are his ISTAR capabilities? Simulation or dissimulation - display or hide? Will it aid display or hide?

Serial	Stage	Considerations
(a)	(b)	(c)
3.	Resources a. ED b. Materiel c. Manpower and equipment	Necessary or not? What? Is it available within timescale? How much? Have I got enough?
4.	Consideration of COA a. How many COA b. Risk assessment c. Selection of Optimum COA	What COA are there (should only be 2 or 3 max) Will I be worse off if deception compromised? Confirm with higher commander. How can I monitor it?
5.	Produce Deception Plan a. Identify friendly activity to cause en to take required action b. OPSEC analysis of above c. Integrate deception and OPSEC plan. d. Distribution	Aim - required en action? How much real activity supports deception plan (the more real activity can be used, the better)? What should the enemy do in reaction to each stage? What must I hide to conceal real activity that could compromise plan? Who needs to know?

INTELLIGENCE REQUIREMENTS FOR DECEPTION

1. Capabilities and weaknesses of the enemy's ISTAR assets, including those of sympathetic nations/organisations.
2. Enemy capability to process and analyse information and intelligence.
3. Capabilities and weaknesses of the enemy's C3I systems.
4. Profiles of key enemy leaders/military commanders, including analysis of their decision-making processes and identification of biases/preconceived perceptions.
5. Historical assessment of enemy susceptibility to deception operations in recent conflicts.
6. Identification of suitable "avenues" to exploit in the deception plan at the operational and strategic level.
7. Current intelligence on enemy ORBAT, deployment, dispositions and intentions, to identify suitable areas for exploitation in any deception plan.
8. Identification of necessary OPSEC measures in support of the deception plan, including enemy ISTAR systems to be neutralised or destroyed.
9. Current intelligence on enemy's ORBAT, force dispositions and any changes/re-deployment as a result of deception operations.
10. Monitoring progress and effectiveness of deception plan.
11. Assessment of enemy's own deception doctrine, tactics/procedures and capability.
12. Counter Intelligence (CI) support to deception operations.
13. Force Protection support to deception operations. CI and Force Protection are particularly relevant to deception measures in rear areas and in OOTW.
14. Possible role of other Government Departments and National Agencies.

REQUIREMENTS FOR DUMMY LOCATIONS

1. Dummy Armoured Company Group Position

Serial	Resources and Time	Requirement
(a)	(b)	(c)
1.	Real Equipment and Manpower.	a. One infantry section to construct the position and remain in situ thereafter. b. The section IFV to make a plausible track plan and provide the electromagnetic signature of an HQ vehicle. c. One MILAN plus IFV main armament to produce direct fire when the position is probed by the enemy. d. One CVR(T) on withdrawal.
2.	Deception Stores.	a. Two dummy tanks and 2 dummy IFVs. Inflatables are preferable to wood and hessian structures as they are less bulky, more plausible and easier to redeploy. b. Camouflage nets. c. Dummy heat sources. d. Trenches dug to 0.3 m with branches or bracken placed in the bottom and spoil only partially concealed. e. Six coils of barbed wire/tape. f. (Optional) Four hundred metres of single wire, posts, tilt rods and 15 minefield markers for a dummy protective minefield. g. Six dummy direction signs. h. Three sets of dummy optics to simulate anti tank weapons. i. Badly (but not grossly so) camouflaged jerricans and ammunition boxes.
3.	Time to construct.	Eight hours (excluding outloading of stores).

2. Dummy Gun Position

Serial	Stage	Considerations
(a)	(b)	(c)
1.	Real Equipment and Manpower.	a. One NCO, 3 men. b. One radio. c. One pistol, or roving gun to provide tracks and fire occasionally in coordination with the remainder of the battery.
2.	Deception Stores.	a. Two dummy guns. b. Camouflage nets. c. Dummy heat sources. d. Firing simulators made from charges placed one metre above the ground to deceive enemy sound ranging equipment. (1.36 kg charge simulates 105 mm gun and 1.8 kg charge simulates 155 mm gun). e. Flash simulators.
3.	Time to Construct.	Two hours. Note that the dummy battery would have to move regularly in order to retain credibility.

3. Dummy Unit CP

Serial	Stage	Considerations
(a)	(b)	(c)
1.	Real Equipment and Manpower.	a. One or two men. b. Two 1-tonne vehicles. c. One generator. d. Camouflage nets.
2.	Deception Stores.	None.
3.	Time to Construct.	Less than 30 mins. Cam nets should be arranged as if covering aerials. Generator or engine left running for noise effect. If the enemy has extensive EW capability, consideration should be given to suitable transmissions.

DECEPTION PLANNING WORKSHEET

1. **Aim of Operation:** X Mech Bde are to attack onto Obj LION in order to defeat 1 MR Bn/17 MR Bde (1).

Factors (from Estimate):

- a. From IPB: terrain hilly and wooded; 3 possible Mobility Corridors (MC) into area (Routes 212, 290, 235).
- b. 17 MR Bde has detached 2 Btys 125 mm Towed A/Tk guns in support 1 MR Bn. These guns need 30 minutes to deploy and conceal in firing positions.
- c. Enemy aware attack likely in next 12 hrs.
- d. Enemy makes considerable use of roads; assumes we do likewise.
- e. Tactical level only enemy ISTAR assets considered.

2. **Aim of Deception Plan:** To cause the enemy to deploy his A/Tk reserve to North of Obj LION.

3. **Friendly COA to Cause Aim:** Own Main Effort along line of Route 235; diversionary efforts only along other MCs.

Indicators	Method/Ruse	Timings (hours)	En ISTAR Capability	En ISTAR Capabilities to Detect Indicators				Desired En Reaction
				Tactical (2)				
				ISTAR Asset	Detect?	Transparent? (3)	OPSEC Measures? (4)	
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)
Increase in recce activity on Rte 235.	Low-level air recce along Rte 235.	H-12	HUMINT	AD, all units.	Yes	No	Covert surveillance on other MCs.	Increased alertness in area Rte 235.
	Poorly concealed Close Recce patrols along Rte 235.	H-11 to H-6		All units in area.				
	Breach of COMSEC by Close Recce.	H-10	SIGINT	Bde Recce Bn SIGINT Coy.	Yes	No	COMSEC for other X Bde units.	Increased alertness in area Rte 235.
			IMINT	N/A				

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)
Establish concentration area near Rte 235.	1. Deception force establishes false bde concentration area using one coy real vehicles plus camouflaged area where others “hidden”.	H-4 to H hr	HUMINT	Bde Recce Bn.	Probably	No if own ground ptls effectively	Implement strict countersurveillance measures elsewhere. Additional ptls in S to deny en recce, “slack” drills in N to allow 1 or 2 en ptls/vehs through.	Enemy focus on N of X Bde area.
	2. Bde Step Up HQ moves into concentration area.			Bn Recce Bn.				
	3. Premature move of Dressing Station and Main Repair Group.			Bde Recce Bn.				
	4. Distribution Point established close to false concentration area.			Bde Recce Bn.				
	Bde Step Up establishes comms.	H-3	SIGINT	Bde Recce Bn SIGINT Coy.	Probably	No - real equipment to be used.	Bde Main HQ and units on radio silence - use of landline.	
Temporary “accidental” relaxation in overhead camouflage in false concentration area.	H-4	IMINT	Tactical Air Recce.	Probably	No - but ensure cam relaxed is over real vehs.	Ensure good overhead cam on real activity.	En confirmatory air recce.	
	H-3							
Picture of build-up in N builds up.	Artillery adjustment on false objective.	H-3	HUMINT	All units in area.	Yes	No - but must be accompanied by other registration so as not to be too blatant.	No	Possible surge of comms activity.
	COMSEC breach in concentration area.	H-3	SIGINT	Bde Recce Bn SIGINT Coy.	Possibly	No	Ensure strict COMSEC elsewhere.	Possible confirmatory recce activity.
	Track marks in concentration area.	H-3	IMINT	Tactical Air Recce.	Probably	No	Ensure track discipline maintained elsewhere.	
		H-2½ to H-2	HUMINT	N/A			Active countersurveillance against enemy ESM and stand off sensors.	
			SIGINT	N/A				
IMINT			N/A					

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)
Activity in concentration area and along Rte 235.	1. Movement of APCs on Rte 235.	H-2	HUMINT	Bde Recce Bn; Bn Close Recce; units in area.	Yes	No		Visible enemy redeployment in area Rte 235. Enemy at high alert state. Redeployment becomes obvious.
	2. Vehicle noise and dust raising.							
	3. Establishment of waiting areas.							
Focus attention on Rte 235.	1. Radio silence except for traffic control net.	H-30 mins	SIGINT	Bde Recce Bn SIGINT Coy.	Possibly	No	No	A/Tk guns redeployed.
	2. Selective switch on air defence and motar locating radar.		IMINT	N/A				
	Diversionsary attack - coy strength							
			HUMINT	All units in area.	Yes	No for initial engagement.	No	
			SIGINT	Bde Recce Bn SIGINT Coy	Yes	No for initial engagement.		
			IMINT	Tactical Air Recce.	Yes	No for initial engagement.		

- Notes:
1. Based on Generic Enemy (Mobile Forces).
 2. These columns are replicated for the Strategic and Operational levels where appropriate; they have been omitted here for presentational reasons.
 3. Transparent = ISTAR Asset may be able to "see through" deception measure.
 4. OPSEC measure available to counter ISTAR Asset.

CHAPTER 5

DECEPTION IN OPERATIONS OTHER THAN WAR (OOTW)

SECTION 1 - GENERAL

1. **Background.** Historically most deception operations have been conducted within the context of regional or general war involving large-scale conventional military forces. However, deception is by no means confined to this type of operation and has been used successfully in most forms of conflict, particularly in large-scale insurgency. The Chinese Communist guerrillas used it in their struggle with the forces of Chiang Kai-sek in the 1930's, (and at the tactical and strategic level later in the Chinese Civil War, 1945 - 49). The Viet Minh used deception in their conflict with the French in Indo-China (1945 - 54), and both their successors the Viet Cong and the US employed it extensively during the period of US involvement in Vietnam (1965 - 72). More recently, the Afghan *Mujahideen* practised deception in their fight against the Soviet invaders (1979 - 89). Deception in OOTW requires consideration of additional factors which are addressed here.
2. **Possible Constraints on the Use of Deception.** For the purposes of this publication, OOTW covers conflicts ranging from peace enforcement to large-scale counter-insurgency operations. Deception has no role in peace support operations, where the principle of transparency is vital and operations have to be manifestly "above board". There could also be circumstances where the government may wish to adopt a more open approach to a conflict in order to maintain the confidence of other parties in its actions, or it may consider that to be seen to be taking what could be interpreted as an underhand or devious approach to operations may hinder subsequent negotiations.
3. **Aims and Scale of Deception.** Unlike regional and general war, the enemy may not be clearly defined. Although deception operations are normally conducted in the context of actual conflict involving UK forces, it is possible that a deception operation aimed at influencing wider perceptions may be mounted, with the intention of deterring conflict. Such an operation may involve, for instance, inducing a perception of friendly omnipotence, by exaggerating friendly strengths or capabilities. Normally this latter type of deception will be approved and directed at the strategic level, although implementation may be a tactical activity. This Chapter therefore addresses deception as part of the conduct of ongoing military operations, where it is more likely to be a tactical activity with limited objectives.

SECTION 2 - THE DECEPTION TARGET

4. **Command Structure.** In regional and general war, the enemy can be expected to have a hierarchical command structure with clear delineation of responsibilities. In an insurgency or similar conflict, the command structure is often more diffuse and although the enemy higher command will have an overall strategy, at the tactical level the fighting may take the form of a series of loosely-connected engagements, typically of company to regimental strength. The enemy commander at whom the deception is aimed is likely, therefore, to be the local unit or regional commander.

5. **ISTAR Assets.** The enemy may lack technically advanced ISTAR capabilities. However, he may receive EW/SIGINT support from third parties. EW sensors, devices such as scanners, radar Intruder Detection Systems, Image Intensifiers, infra-red detectors, military-frequency radios and mobile phones are available commercially or from third parties and can be expected in most theatres. In addition to any technical devices, the enemy will frequently possess a complex and sophisticated HUMINT network. Often the belligerent parties will have agents or sympathisers in the other parties' camps and amongst the indigenous population working with friendly forces. This poses security problems, but also offers avenues for exploitation as part of the deception plan. The extent and coverage of these networks, and the likely presence of the indigenous population, will impose constraints upon deception measures. Simulations have to be capable of withstanding close visual scrutiny, as must camouflage and concealment. However, much greater use can be made of "leaks" and other verbal methods of passing information to the enemy.

SECTION 3 - DECEPTION TECHNIQUES

6. **General.** All the deception techniques and types of activity for regional and general war are applicable for OOTW. This Section does not attempt to illustrate every deception technique or activity; rather it aims to show what can be achieved by original thinking, often at short notice and with limited resources.
7. **The False Routine.** In Vietnam a US brigade detached two infantry battalions to support an operation outside its AO. To prevent the Viet Cong (VC) exploiting this weakness, ie to cause them to continue with their low level of activity, a deception was implemented to convince them that US strength had actually been increased by simulating the routine of the arrival of another formation. Support personnel wore the insignia of another division, and put that division's markings on some vehicles. A rumour that this division was to occupy the AO was spread, and groups of personnel wearing the false markings visited fire bases, simulating advance parties. This deception worked until the two battalions returned. Other deception ploys of this nature could include establishing, say, an ambush position under the guise of routine patrolling, but leaving one or two men behind from each patrol.
8. **The Lure.** The lure, possibly combined with the false routine and the deliberate leak, has been used with great effect in the past. The lure technique, often the creation of an incident to lure follow-on forces into an ambush, has been used by almost all guerrilla/insurgent at the lowest tactical level, to entrap patrols or even individuals. The Viet Minh, VC and the US used this technique on a much larger scale. During Op EL PASO, July 1966, the US 1st Div lured VC 272nd Regt into attacking a superior force. Having covertly reconnoitred possible VC ambush sites, they intentionally leaked details of a supply convoy with limited protection. Pre-positioned artillery was laid on the potential ambush sites, with close air support (CAS) kept on station. When the convoy was attacked, a combination of fire from the tracked vehicles inserted in the convoy, artillery and CAS fixed the VC for infantry attack. The Afghan *Mujahideen* used dummy supply caravans to lure Soviet *Spetsnaz* (Special Forces) units into ambushes.

CHAPTER 6

COUNTERING DECEPTION

SECTION 1 - THE POSSIBILITY OF BEING DECEIVED

1. Commanders should always be prepared for the probability of an enemy's deception operations. Some nations, e.g. those of the Former Soviet Union, gained much hard-won experience from fighting on the featureless plains of Eastern Europe, which taught them to place a greater emphasis on deception than on the use of ground as a means of achieving surprise. They have incorporated deception (in the form of *Maskirovka*; see Annex A) at the heart of their military doctrine and can be expected to use it as a matter of course. The Soviet experience is not unique; many nations familiar with desert warfare have arrived at the same conclusion. The Iraqis employed deception successfully in the Iran-Iraq War, 1980-88; as did the Egyptians in 1973. Staff officers from other nations trained in the Former Soviet Union can also be expected to have an understanding of the importance of deception. The Chinese and North Koreans conducted successful deceptions during the Korean War (1950-53). As mentioned in Chapter 5, deception is not solely the province of conventional armies; many insurgent forces have used it. In countering deception, there is no substitute for knowledge of the enemy: his doctrine, recent history, personalities, technical capability (particularly C3I and EW systems); and *modus operandi* at all levels. This is not just a G2 staff responsibility, but that of all commanders.

SECTION 2 - COUNTERMEASURES

2. **General.** Deception is central to many nations' concepts of operations. Just as commanders should consider deception as an integral part of all operations, so should they expect it to be used against them as a matter of routine. Therefore, equal attention needs to be paid to methods of countering the threat. A good defence against deception is to apply the principles of deception in reverse.
3. **Clear Aim.** Deception has to have a clear aim that supports the real operational plan. Does the emerging enemy picture support his perceived operational/strategic and long-term aims?
4. **Centralised Control and Staff Co-ordination.** Successful deception demands a high degree of co-ordination and co-operation between staff branches in its planning, execution and monitoring. Real activities need to be integrated with deceptive ones. Any indications of uncoordinated activity should be looked for:
 - a. Do the enemy's actions appear co-ordinated across his whole force?
 - b. Are there disparities between neighbouring formations?
 - c. Are certain events followed by an unusual level of enemy ISTAR activity (monitoring)?

- d. Are his physical actions consistent with PSYOPS, media and diplomatic messages?
- 5. **Preparation.** Deception measures normally require extensive preparation and allocation of tasks, to allow the events being portrayed to occur in a realistic manner:
 - a. Does the build-up of the enemy picture “flow”?
 - b. Are there unexplained gaps or delays in the build-up of his activities?
 - c. Does his ISTAR activity conform to expected patterns, or is undue attention paid to certain friendly activities or certain areas of the battlefield?
- 6. **Accurate Intelligence.** Deception is founded on accurate and timely intelligence on the enemy. The key to countering deception is also “know your enemy”. Intelligence requirements to support counter-deception are similar to those for deception itself. They are described in more detail at Annex B.
 - a. Does the perceived pattern of activities conform to the enemy’s doctrine and what is known of the commander and his background?
 - b. Does it conform to the enemy’s assessed intentions and what he could reasonably be expected to know about friendly intentions? Equally, be suspicious if enemy actions appear to match expectations too perfectly.
- 7. **Timing.** Timing is critical to deception:
 - a. Does the build-up of activity conform to expected timescales?
 - b. Do the intervals between linked activities match previously observed “norms”?
 - c. Are some activities taking too long (to make sure that they are observed) or too rushed (to prevent detailed observation and analysis)?
- 8. **Credibility.** Deception should not appear illogical and should accord with a pattern of events the enemy has reason to expect:
 - a. Does the unfolding enemy picture make military sense?
 - b. Does it accord with friendly expectations?
 - c. Be suspicious of a too perfect match of expectations.
- 9. **Corroboration.** Considerable effort by the deceiver is required to implant a ruse which is confirmed by all or even most ISTAR systems. Still more effort is required to sustain a ruse over lengthy periods of time. The deceiver may have neither the skill, nor the resources, nor the will to execute his plan with sufficient thoroughness to fool a competent enemy. Sooner or later, through bad execution or bad luck, some

aspect of the deception will be inadvertently compromised. Defence against deception thus requires active and sustained questioning of evidence, searching for corroboration by all available sources and a review of previous deductions as fresh evidence is produced. In particular it is helpful to look for small and obscure details which the deceiver may have omitted, such as the shadows cast by projecting handles and bolts, which may be omitted on a dummy tank.

- a. Has an activity or indicator been detected by a single ISTAR source or agency (eg EW)?
 - b. Has the activity been corroborated by another ISTAR asset operating in a different sensory domain (eg IMINT)?
 - c. Has the activity been confirmed by a fine grain ISTAR system?
 - d. Does the flow of indicators accord to expectations, or has the enemy not apparently implemented effective OPSEC?
10. **Security.** Just as security is vital in implementing friendly deception, so it should be for an enemy deception:
- a. Has any deviation from expected enemy security patterns been observed, particularly inconsistent application of OPSEC and security between units/formations?
 - b. Has information derived from apparent lapses in security been checked/confirmed by other ISTAR means?
11. **Flexibility.** The absence of flexibility may be an indicator of deception: having begun the implementation of a complex plan, the enemy may be loath to change it and his continuance on a particular COA despite changes in the situation should arouse suspicions.
12. **Other Factors.** As well as the specific aspects above, commanders and intelligence staffs should incorporate into their analytical processes:
- a. *An Open Mind.* Ruses are more readily accepted when they conform to a preconceived idea in the mind of the target. The ingredients of the ruse appear to be feasible and logical because they are more or less what the target is expecting. The counter is to suppress preconceived ideas and retain an open mind.
 - b. *Scepticism.* Analysts should be reluctant to accept evidence at face value and should be automatically suspicious of information which has not received the protection of routine security precautions.
 - c. *Resistance to Jumping to Conclusions.* There is constant pressure on intelligence staffs to reach conclusions and formulate predictions. There are deadlines to be met for the timely dissemination of their intelligence. Shortage of

time often precludes an exhaustive collection of evidence. It is on such conditions that the deceiver thrives. Commanders and G2 staffs on the other hand have to resist the temptation to jump to conclusions.

- d. *Attention to Anomalies.* Deception plans are seldom flawless. Indications of false activities can be clumsily presented and indications of genuine activity can rarely be totally suppressed. Analysts are frequently confronted by a proportion of incongruous detail which should not be lightly dismissed as the result of inaccurate or mistaken reporting. Anomalies, which might prove to be the flaw in an otherwise convincing pattern, must be subjected to the same routine of double checking as other evidence.
- e. *Adherence to Intelligence Procedures.* Short circuiting of intelligence procedures greatly assists the deceiver. The proper procedures for processing information by collation, evaluation, analysis, integration and interpretation must be adhered to. A similar adherence to the Intelligence Preparation of the Battlefield (IPB) process is essential.

MASKIROVKA

1. **Introduction.** Deception and surprise were, in the Soviet mind, inextricable. Surprise was seen as a vital precursor to success, and *Maskirovka* the means for achieving this. It is defined as:

A complex of measures, including concealment, simulation, camouflage and disinformation, to mislead the enemy as to: the presence or deployment of forces and targets (equipment and installations); their subordination; combat readiness and their activity; and also the commander's plans, the aim of the operation or battle. *Maskirovka* contributes to achieving surprise, security and combat capability and applies at all levels from sub-unit to strategic¹.

2. **Concept of *Maskirovka*.** The concept of *Maskirovka* embraces all concealment, deception and misinformation techniques and is derived from a study of experience. It was an essential element of Soviet planning at all levels and is described as a branch of Military Art. It evolved over a considerable period and was developed still further as a result of Soviet experiences in the Great Patriotic War (WW2). Its importance continues to be emphasised in current Russian military writings, and has been taught to several generations of other nation's staff officers trained in Soviet military institutions. It is a concept that fitted easily within a society where secrecy was almost instinctive. *Maskirovka* is associated with all strategic, operational and tactical activities, depending on objectives, scope and the way in which operations are conducted. The key point remains that it is a dynamic concept and it is always given prominence at the earliest stages of the planning process.
 - a. **Strategic *Maskirovka*.** *Maskirovka* at the Strategic level is the series of measures and actions organised and carried out at national and theatre level in the military sphere and in the political, economic and diplomatic spheres. The ultimate aim is the achievement of particular political and military objectives, confusing and misleading any potential adversary by disguising true political and military intentions.
 - b. **Operational *Maskirovka*.** *Maskirovka* at the Operational level is the series of measures and actions designed to conceal operational objectives, the location of the enemy's probable reconnaissance targets, and to mislead the enemy about the strength and deployment of the main groupings of forces. It is directed at Front level and usually calls for specialist forces and resources.
 - c. **Tactical *Maskirovka*.** *Maskirovka* at the tactical level is applied to measures adopted by divisional-sized formations and those taken at unit level and prima-

1. Soviet Military Encyclopaedic Dictionary, 1986.

rily embraces the techniques of camouflage. In most cases it does not call for specialised forces and resources but relies instead on drills and procedures which formed part of the standard basic training of the Soviet soldier.

3. **Objectives of Maskirovka.** *Maskirovka* at the operational and strategic level is carried out in peacetime, as well as in war, and is considered an important factor that helps to ensure surprise, promote the effectiveness of combat actions, and maintain the combat power of troops and fleets. *Maskirovka* is the combination of a series of measures co-ordinated in terms of objective, time, and space, and directed to deceive the enemy as to:
 - a. Plans and intentions of the Soviet friendly forces' command.
 - b. Composition of forces and means.
 - c. Disposition, status, and combat capability of friendly forces and means, and the nature of their actions.
4. **Methods.** Different methods and forms can be employed to achieve *Maskirovka*. The principle methods are:
 - a. *Secrecy*: eliminating or limiting the disclosure of indicators of friendly forces and their actions; strict COMSEC; limited distribution of plans.
 - b. *Deception*: setting up dummy targets and deceptive situations concerning the actions of friendly forces; the use of mock-up and decoy equipments, structures and facilities.
 - c. *Imitation and Pretence*: demonstrating deliberate actions by real forces to lure the enemy.
 - d. *Dissemination of Deceptive Information*: giving false and deceptive information to the enemy.
 - e. *EW*: technical interference with enemy ISTAR; normally intrusion on to enemy radio nets and links.
 - f. *Camouflage and Concealment*: the exploitation of terrain, night and weather conditions to conceal deployments; the use of smoke, netting, local materials and screens; sound and light discipline.
5. **The Rewards.** The success of *Maskirovka* is achieved through:
 - a. Taking detailed and timely measures integrated in a pre-arranged plan.
 - b. Exercising systematic and centralised control of *Maskirovka* arrangements. *Maskirovka* operations must be continuous and through all levels of command.

- c. Ensuring the secrecy of the *Maskirovka* plan.
 - d. Ensuring the dynamism, credibility, and continuity of *Maskirovka*.
 - e. Making timely decisions and taking timely measures in support of *Maskirovka* before and during military action.
6. ***Importance of Maskirovka.*** The Soviets considered *Maskirovka* to be so important that it was a mandatory element in all planning, from strategic down to sub-unit level. Up to a third of all troops involved in an operation could be assigned to *Maskirovka*. *Maskirovka* has to be persuasive or plausible as the enemy is unlikely to waste his resources on decoys or dummies that do not deceive. It should be varied or diverse; if *Maskirovka* is stereotyped or repetitive, it is unlikely to conceal or deceive.

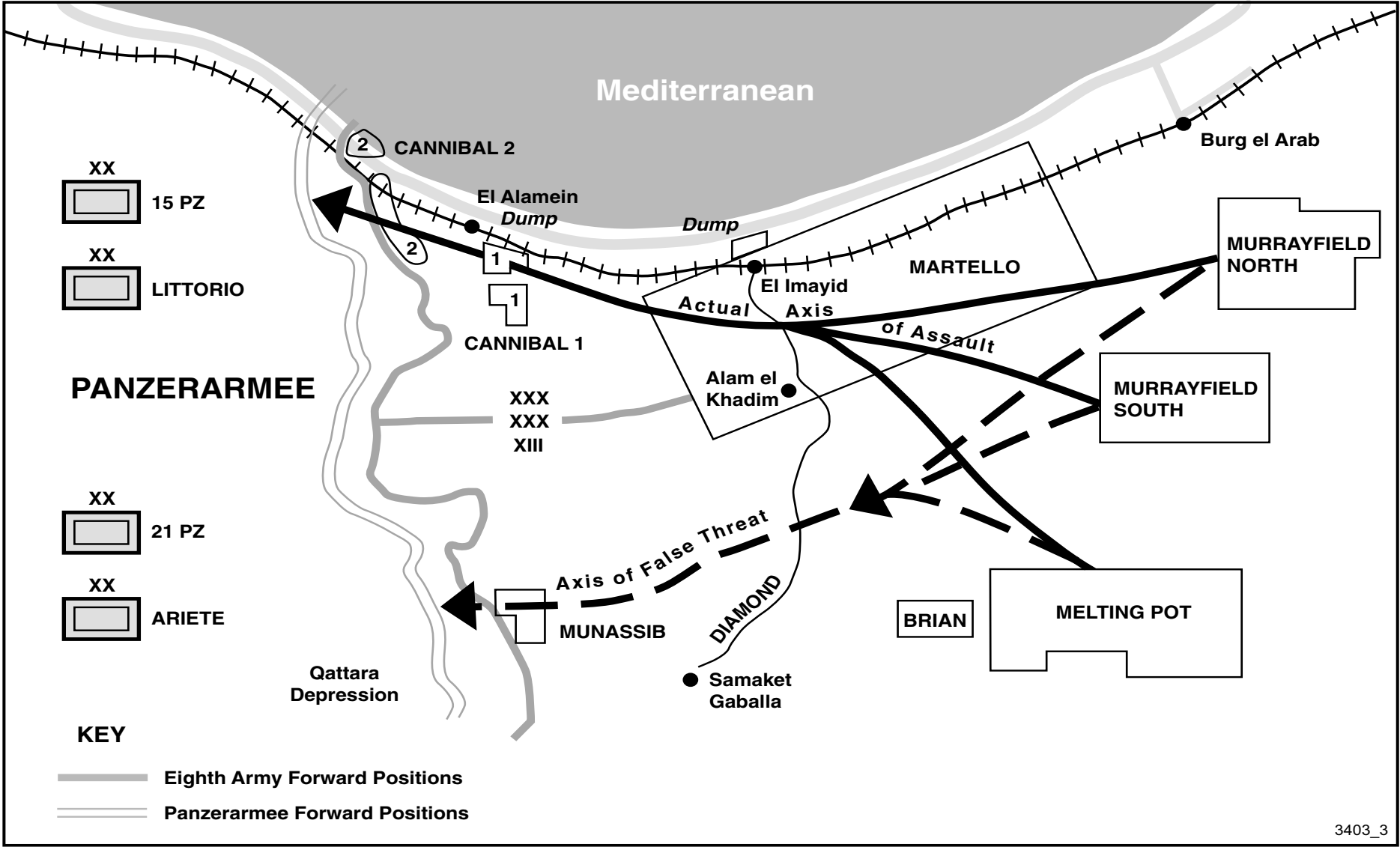
INTELLIGENCE REQUIREMENTS FOR COUNTER-DECEPTION

1. Profiles of key enemy leaders/military commanders, including analysis of their decision-making processes and studies of their career history and experiences.
2. Historical assessment of enemy use of deception in recent conflicts.
3. Assessment of enemy's own deception doctrine, tactics/procedures and capability.
4. Current intelligence on enemy ORBAT, deployment, dispositions and intentions, to identify possible anomalies in the perceived picture.
5. EW: detailed analysis of SIGINT to identify anomalies between electro-magnetic emissions and ground activities.
6. Multi-sensor IMINT: to provide corroboration of SIGINT and optical "sightings".
7. Capabilities of the enemy's ISTAR assets, including those of sympathetic nations/organizations.
8. Capabilities and weaknesses of the enemy's C3I systems.
9. Enemy's capability to process and analyse information and intelligence. These latter two capabilities will indicate the enemy's capability to monitor the results of his deception - and thus allow friendly forces to turn a (detected) enemy deception operation to their own purposes.
10. HUMINT from Prisoners of War (PWs) and deserters: it may be necessary to mount special raids to take prisoners to confirm (or otherwise) the perceived picture.
11. Identification of necessary OPSEC measures, including enemy ISTAR systems to be neutralised or destroyed, to prevent the enemy from ascertaining the success or otherwise of his deception.
12. Counter Intelligence (CI) support to monitor and disrupt enemy covert activity: thus hindering enemy monitoring of the success (or otherwise) of his deception plan.
13. Force Protection support to counter-deception operations: CI and Force Protection are particularly relevant to counter-deception in rear areas and in OOTW.
14. Possible role of other Government Departments and National Agencies: in particular these may have access to high-level HUMINT.

PART D

HISTORICAL SUPPLEMENT

OPERATION BERTRAM, WESTERN DESERT 1942



CHAPTER 1

OPERATION BERTRAM. WESTERN DESERT 1942

General

1. Operation BERTRAM was the deception operation supporting Montgomery's decisive attack at El Alamein in North Africa in 1942. It is a good example of successful deception at the operational level.
2. Op BERTRAM worked on the principle that strategic surprise was impossible, as Rommel was expecting an attack after his defeat at Alam Haifa; therefore the aim was to deceive him as to the date and location of the main attack. The Axis forces had no preconceived idea when or precisely where; Op BERTRAM had to provide that information. The deception plan for El Alamein was masterminded by Lt Col Richardson¹ and implemented by "A" Force, the deception organisation for the Middle East. At El Alamein Montgomery planned to attack the Axis forces in the North. The aims of Op BERTRAM were threefold:
 - a. To cause the Axis forces to take a specific action, in this case to divert forces from the North, and tie down the two divisions in the South, by deceiving the Axis forces into believing that the main attack would come in the South.
 - b. To cause him to continue on his existing course, in this case to continue his defensive preparations at the same rate, by indicating that D-Day would be 7 Nov 42 (the real date was 23/24 Oct).
 - c. To cause him to do nothing at all, in this case to delay committing his armoured reserves until at least D+4, by creating uncertainty in his mind as to subsequent objectives.
3. Op BERTRAM had to be maintained for some seven weeks, but this included vital all-arms training for X Armd Corps 1st and 10th Armoured Divisions and 24th Armoured Brigade to correct the deficiencies exposed in earlier battles. This training was fully integrated into the deception plan.
4. Throughout WW2 the Allies had access to ULTRA intelligence, obtained from decrypts of German top level signals traffic. This gave them excellent insights into what senior German commanders knew and what they were thinking. During 1942 the Germans had the three main forms of intelligence:
 - a. HUMINT, in the form of occasional PWs, but more importantly, a spy network operating throughout the Middle East.
 - b. IMINT, in the form of photo recce missions.

1. Later General Sir Charles Richardson.

- c. SIGINT, the interception of tactical and operational comms traffic.

Disinformation at the Strategic Level

- 5. Op BERTRAM, the operational plan, was supported by Op TREATMENT, at the strategic level. The first step in TREATMENT was false information fed into the Axis espionage networks known to be operating in Cairo and throughout the Middle East. Rumours were leaked from the British Embassy in Cairo and other sources that Montgomery's attack was scheduled for a moonless night on 6/7 November. Further disinformation was put about that the new Shermans arriving in the Middle East were suffering from technical desertisation troubles and would not be fit for service until November. A bogus conference was arranged for 26 October in Teheran to be attended by Alexander, CinC MELF and other senior commanders. The officers and their ADCs were just a little indiscreet in booking air passages and accommodation. Some well publicised cocktail parties and Nile boat trips were organised for late October.

The Southern Bait

- 6. Returning to the operational plan, concealment in the desert was virtually impossible and reliance had to be placed on disguise and deception. During September and the first half of October, X Armd Corps' exercises took place in the southern half of the area between the Mediterranean and the Qattara Depression with the accent on movement in a southwesterly direction - using real activity as part of the deception plan. Although 8th Armoured Division had been disbanded to make the other armoured divisions up to strength its headquarters was retained in the South to broadcast bogus signals traffic. 7th Armoured Division was also stationed in the South to launch a holding attack.
- 7. A water pipeline already ran from El Imayid railway station near the coast SSE to the Alam el Khadim area. A dummy pipeline, codenamed *Diamond*, was laid in a SSW direction to Samaket Gaballa, 20 miles further on, at a rate which gave the impression of a completion date still nearer the southern sector of early November. Stretches of trench were dug and lengths of dummy pipeline, made from old four-gallon petrol cans, were laid alongside it. At night the trench would be filled in and the dummy pipelines carried forward to the next stretch.
- 8. A few miles to the east of Samaket Gaballa a nine mile square patch of desert, codenamed *Brian*, was made to look like a dump containing 9,000 tons of combat and engineer supplies by building 700 dummy stacks. One of the armoured exercises in the southern area caused the builders some concern but left a realistic pattern of wheel and track marks. Work on *Brian* started on 7 October and finished a fortnight later.

The Northern Hoax

- 9. During the night of 18/19 October and the following day, X Corps concentrated its armoured formations quite openly in three staging areas, *Murrayfield North* and

South, and *Melting Pot*. They looked like any concentration area for an exercise but were carefully located where the track patterns ran in a south-westerly direction towards the southern sector, thus helping to portray this picture.

10. The real assembly area for X Corps, *Martello*, was to be further forward in the northern sector within an easy 15 to 20 miles of the intended point of attack. There could be no hope of hiding such a concentration in an area 12 miles by 8 and so it was decided to establish a pattern, over three weeks in advance of D-Day, which Axis reconnaissance aircraft and intelligence would get used to and accept as something not out of the ordinary. Transport from base and LofC units was brought in to the area and dummies added to bring the total number of vehicles or substitutes to equal the total in X Corps.
11. Two years earlier, Wavell had suggested the manufacture of quickly detachable wheeled vehicle dummies, which could be used to disguise tanks. 722 *Sunshields*, as they were nicknamed, were delivered to *Martello* where they were placed in the precise positions to be occupied by X Corps' tanks. Each hide was given a serial number, which corresponded with the serial number given to an individual tank crew. The crews were sent up to *Martello* in trucks which appeared to be part of the normal maintenance traffic and shown where to go when they moved up on the two nights before D-Day, 20/21 and 21/22 October.
12. A number of tracks had to be constructed between the staging areas and *Martello* to allow X Corps' night moves forward to go without a hitch. The problem was that the tracks would give away the direction of Montgomery's thrust near the coast. The solution was to plan the routes from a combination of ground reconnaissance and air photography to choose terrain where engineer work would be least conspicuous. Having decided on the lines the tracks were to take, the engineers began work at different, and to start with, apparently unrelated sections of the track. Only when the sections were joined up just before D-Day was the pattern clear. Then reliance was placed on intercepting enemy reconnaissance aircraft.
13. The move went without a hitch. As the tanks and trucks left the *Murrayfield* and *Melting Pot* staging areas, dummies replaced them to present Axis air reconnaissance with a consistent picture. Similarly, the vehicles which had been sitting in the *Martello* assembly area for three weeks, were withdrawn as X Corps' trucks took their place.

Hiding the Artillery and a Double Bluff

14. Concealing the 400 field and medium guns concentrated in assembly areas behind the front and in their eventual gun positions was solved by erecting a dummy canopy over the 'quad' gun-towers, which had a distinctive shape, and their 25 pounders and limbers. Gun and limber were backed up together with the limber's pole overlapping the gun's trail to produce the pattern of a four-wheel vehicle. The dummy canvas tops, called a *Cannibal*, because it swallowed the real equipment, completed the disguise. The assembly areas and the gun position areas were accordingly dubbed *Cannibal 1* and *Cannibal 2*. The disguise was only thrown off after dark on the night of the attack.

15. In the centre and southern sectors dummy artillery, camouflaged well enough to disguise its bogus nature, was set up to compensate for the artillery concealed by *Cannibals* in the north. In the Munassib Depression a double bluff was organised to support 7th Armoured Division's holding attack and Headquarters 8th Armoured Division's simulated attack to prevent 21st Panzer and Ariete from reinforcing the sector in the north where the real blow was to fall. Three and a half field regiment's worth of dummy guns and vehicles were set up in *Munassib*. A special effort was made to give a good imitation of normal activity and not to make the camouflage too perfect. A few days before the attack, the camouflage maintenance was allowed to lapse so that Axis air reconnaissance would discover their true nature. At the last minute the dummies were replaced by real guns to support 7th Armoured Division's holding attack. Although the attack was held up after penetrating the screen and the first Axis minefield, the surprise added to the credibility of the feint.

Hiding the Supply Dumps

16. Then there was the task of concealing 6,000 tons of combat supplies in two large dumps, one at El Alamein Station and the other near El Imayid Station 15 miles to the east. At El Alamein the problem was how to hide the main petrol dump. Fortunately the area had been prepared for defence with well constructed, stone-revetted trenches. A layer of petrol cans was stacked up against each wall of a trench so that the internal shadows looked virtually unchanged from the air. The RAF was invited to look for the hidden cache and failed to do so. Rations were stacked in piles shaped like 3-ton trucks and camouflaged at the standard 150 yard spacing between vehicles. Small quantities of stores were disguised to look like bivouacs. Traffic was deliberately diverted through the dumps to simulate realistic activity.

The Result

17. The deception was a complete success. All three aims were achieved fully or in the main and as history relates, Montgomery won a decisive victory at El Alamein.

Op BERTRAM and OPSEC

18. Op BERTRAM shows the importance of seemingly unimportant details to the OPSEC plan without which deception is likely to fail. At a conference on 21 Oct 42 the Chief G2 from OKH (the German High Command) expressed the opinion that the decisive British attack would not begin until early November - as Op BERTRAM had portrayed. However, on 15 Oct, G2 Afrika Korps intercepted and decrypted a demand for additional stretcher-bearers for the 8th Army. Previous experience had shown that such demands were submitted eight days before an attack, putting the date for the attack as 23 Oct, the planned date. Fortunately, because of other, contradictory, evidence this information was not acted on.

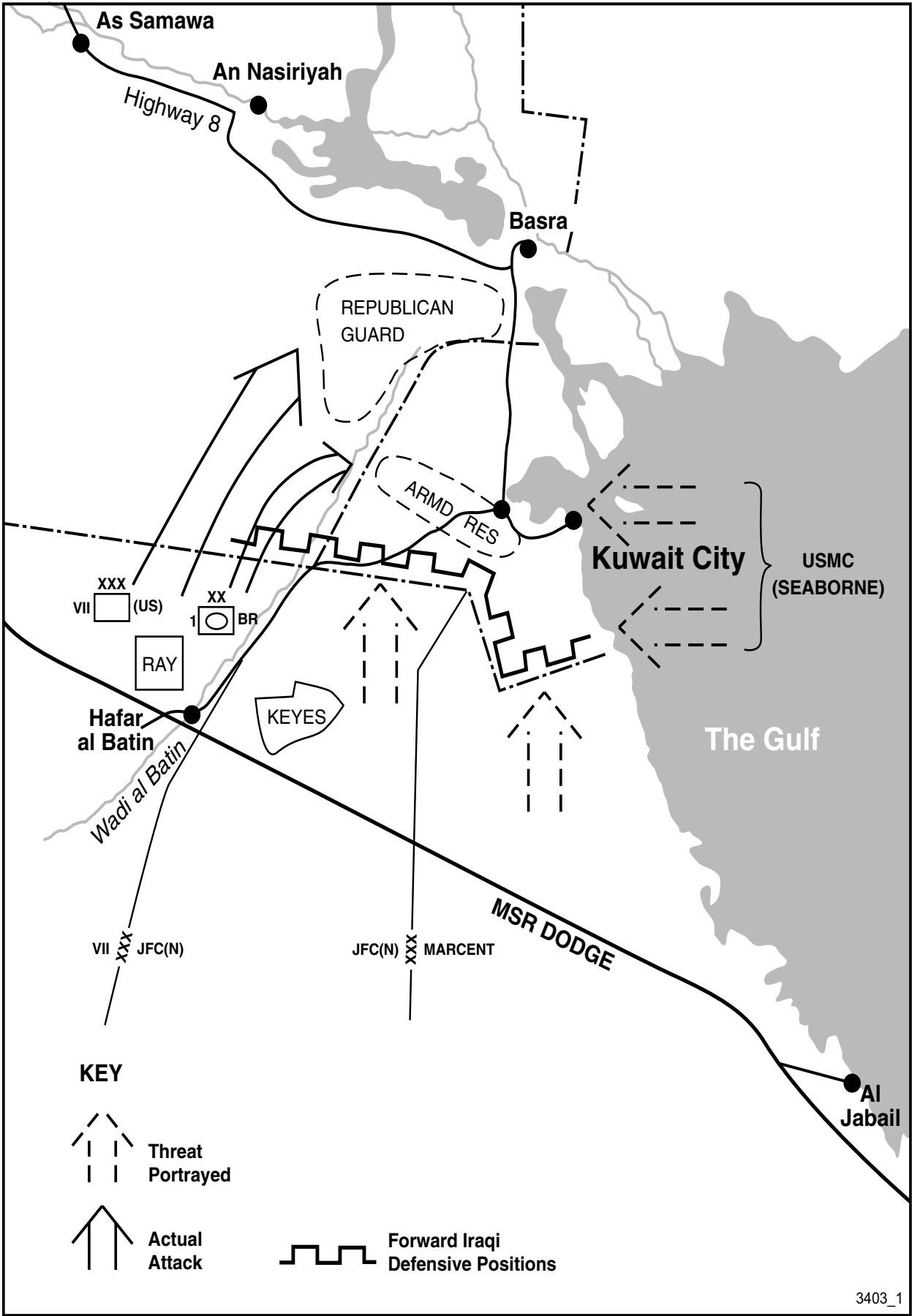
Summary

19. Op BERTRAM had a clear aim, albeit threefold: to cause the enemy to maldeploy his forces; proceed with defensive measures at a rate which would ensure that they were

incomplete by the time of the attack; and to withhold his reserves until their committal would be relatively ineffectual. All of these were clearly prejudicial to his interests, and directly supportive of the real plan. It also demonstrates the potential complexity of an operational deception.

20. Op BERTRAM demonstrates that real events (X Corps training) can be integrated into a deception, reducing the deceptive effort needed and, at the same time, reducing the risk of compromise; nothing is as realistic as the real thing.
21. The importance of OPSEC to a deception plan is shown. Active OPSEC was involved (the interception of Axis reconnaissance aircraft in concealing the tracks for X Corps's night moves); as was OPSEC monitoring (the RAF reconnaissance overflights of the combat supplies dumps at El Alamein Station and El Imayid Station). Finally, the importance of seemingly minor details is demonstrated, as in the potential compromise of the whole deception plan by the interception of logistic traffic in the form of requests for additional stretcher bearers.

OPERATION DESERT SABRE, THE GULF 1991



CHAPTER 2

OPERATION DESERT SABRE. THE GULF 1991

The Operational Setting

1. In 1990 Iraq invaded Kuwait. An international Coalition Force incorporating 1 (BR) Armd Div was formed to assist in the implementation of the UK Security Council's resolutions to restore Kuwait's sovereignty. This Chapter does not attempt to describe the whole campaign; only the part played by 1 (BR) Armd Div in the ground deception plan that formed part of the overall operation.
2. 1 (BR) Armd Div, under Maj Gen Smith¹ was resubordinated from MARCENT (US Marines) to VII (US) Corps on 14 Dec 90. VII (US) Corps in turn was part of US CENTCOM, commanded by Gen Norman Schwarzkopf. CENTCOM's plan, nicknamed Desert Sword, centred on tying down the entrenched main forward Iraqi ground forces whilst attacking round them West of the Wadi Al Batin to take on the Iraqi Republican Guards, deployed North of Kuwait. The well-equipped Republican Guards were the operational focus and their defeat, surrender or retreat was the Coalition Main Effort.

The Deception

3. The deception involving VII (US) Corps and 1 (BR) Armd Div was part of a strategic deception which was to persuade the Iraqis to reinforce their defences along the Kuwaiti coast and the Southern Kuwait/Saudi border.
4. The friendly activity to cause this was a combination of the considerable US Marine Expeditionary Force off the Kuwait coast and the main weight of land forces deployed South of Kuwait, East of the Wadi Al Batin. This would lead the Iraqis to conclude that the main attack would come from the sea, supported by a land attack directly North into Kuwait. 1 (BR) Armd Div's aim was to disguise the fact that it had been resubordinated to VII (US) Corps.
5. 1 (BR) Armd Div's deception had three main strands:
 - a. *EW*. From 7 – 24 Jan 91, EW assets monitored and recorded the Div's VHF, HF and HF Radio Adaptive Telegraph Transmission (RATT) nets. The VHF recordings were not of sufficient quality to be played back, but this was unimportant as the Iraqis did not possess ground ESM with a sufficient range (all Iraqi airborne EW assets had been grounded by the air war). From 26 Jan to 6 Feb the recordings were played back using four transmitters, to maintain the picture that no significant developments were occurring. The success of this deception was confirmed by Iraqi attempts to jam these transmissions.

1. Later General Sir Rupert Smith.

- b. *Movement, Deployment and Training.* The aim of the deployment into Concentration Area KEYES were to make the Iraqis think that only unimportant training movement was occurring along MSR DODGE. This was achieved by an early move of logistic assets intermingled with the heavier movement of US forces prior to the move of the rest of the Div to KEYES. Concealment of the move was aided by OPSEC. Effective active OPSEC measures prevented Iraqi air and ground reconnaissance approaching the area, which was also out of range of Iraqi HUMINT, whilst passive OPSEC measures included EMCON. Movement into KEYES was largely completed by 1 Feb 91. EW assets continued to monitor radio traffic and transmit recordings until 23 Feb.
 - c. *Artillery Fire.* During the period 14 – 24 Feb the Divisional Artillery Group was sent up to the Kuwaiti border to carry out artillery raids. Part of the purpose behind these raids was to add weight to the deception by indicating that a frontal attack was being planned.
6. 1 (BR) Armd Div began its move from KEYES to Assembly Area RAY on 16 Feb, and by 23 Feb was ready for the commencement of the attack on the following day. Had its move to RAY been detected by the Iraqis the deception would still have achieved its aim as by then they had deployed their forces and expended the majority of their defensive stores; in other words, it would have been too late to redeploy to meet any other than the frontal one they were expecting.
 7. Rhino Force was a tactical deception plan. 1 (BR) Armd Div, as a two-brigade formation, had no real reserve. The concept, therefore, was to simulate a brigade which would fix elements of the Iraqi Republican Guards whilst 4 Armd Bde redeployed during the main land battle that commenced on 24 Feb, but in the event it was not used. It consisted of four Westlands Large Area Smoke Screen Trailers and four US PSYOPS loudspeaker detachments. In the event of its committal, it would have received a mixed battlegroup bolstered with extra radios from 7 Armd Bde. The aim was to create the smoke, dust and noise of a full brigade, whilst 7 Armd Bde's remaining battlegroups would use 2-dimensional dummy tanks to fill the gaps in their ranks.

The Result

8. The deception was a success. The Iraqis were mal-deployed to meet the attack when it came. The ground battle lasted only four days, from 24 – 28 Feb, and resulted in total victory for the Coalition.

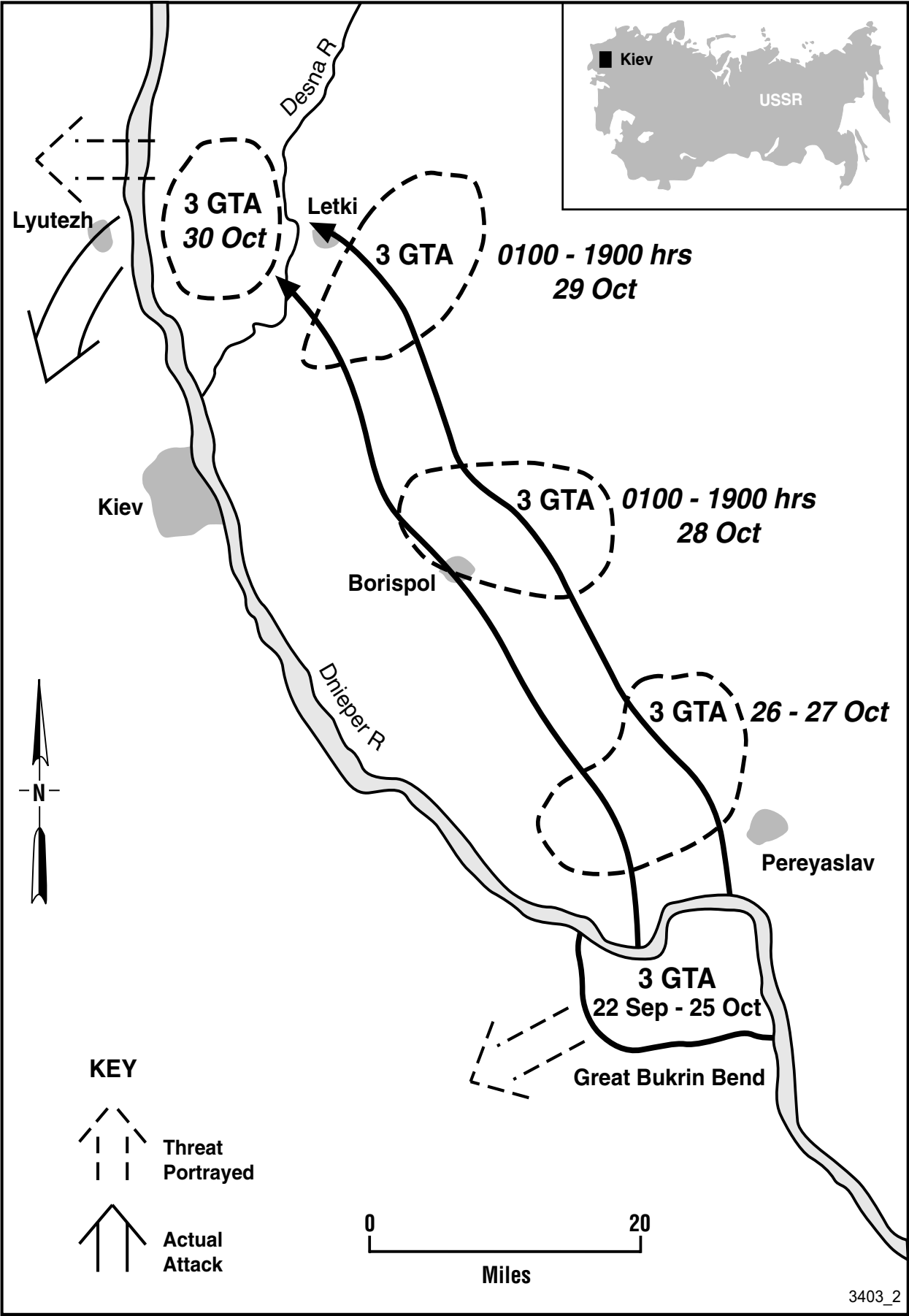
Lessons from DESERT SABRE

9. 1 (BR) Armd Div's deception was part of a wider, strategic plan. In isolation it would have achieved little or nothing, and reinforces the principle of centralised control. It was achieved with very few resources (mainly EW), and the artillery fires served the dual purpose of furthering the deception and destroying Iraqi forces. However, a major contribution to its success was the Coalition total control of the air, without which the deception would have been much harder to implement. Had the Iraqis had

an airborne reconnaissance capability, much larger resources, such as realistic dummies, would have been necessary. Similarly, the Iraqi reluctance to conduct aggressive armoured reconnaissance, coupled with effective Coalition counter-reconnaissance, made implementing the plan much easier. The nature of the desert terrain denied the Iraqis the opportunity to deploy or use HUMINT in the area of KEYES.

10. Rhino Force demonstrates the potential for relatively simple tactical deception measures. Although not used, it is probable that it could have worked and gained 4 Armd Bde the vital time needed to redeploy. In a fast-moving battle, a few minutes extra time can make the difference between success and failure.

THE RE-GROUPING OF 3 GUARDS TANK ARMY, UKRAINE 1943



CHAPTER 3

THE RE-GROUPING OF 3 GUARDS TANK ARMY. UKRAINE 1943

The Strategic Setting

1. This example is taken from the Eastern Front during WW2. The Soviets were masters of *Maskirovka*, which includes deception, and the movement of 3 Guards Tank Army (GTA) in the Kiev area, although an operational deception, has many lessons at the tactical level.
2. Following the failure of the German Kursk offensive in July 1943, the Soviets took the initiative, and by the end of September 43 had reached the River Dnieper on a 700 km front from Loyev to Zaporozh'ye, with 23 small bridgeheads on the western bank. One of these, South of Kiev, was secured by the Voronezh *Front* (shortly afterwards renamed the 1st Ukrainian *Front*) and was known as the Great Bukrin Bend. Despite repeated failures to break through the German positions (which included a surprise airborne assault), Vatutin, the *Front* Commander, had been able to move significant forces into the bridgehead, including major elements of 3 GTA.
3. A further attempted breakout in the Bukrin area failed. However, this operation succeeded in concentrating the Germans' minds on Bukrin and allowed 38 Army to enlarge its bridgehead around Lyutezh. Vatutin's plan for a new *frontal* offensive involved widespread activity in both the North and South of his sector, with supporting attacks by the flanking Central and Steppe *Fronts*, to tie down the Germans whilst he carried out two major regroupings to concentrate his forces for a breakthrough in the Lyutezh area.
4. Part of this plan involved the move in secret of 3 GTA from the Great Bukrin Bend North to Lyutezh (the Germans knew 3 GTA was at Bukrin). At 1830 hrs on 25 Oct 43 Vatutin assigned 3 GTA (along with supporting formations) the mission of withdrawing from the Great Bukrin Bend, marching North, and occupying jump-off positions for an offensive from the Lyutezh bridgehead.

The Deception

5. 3 GTA had to be in position for an attack planned for 1/2 Nov (subsequently delayed to the 3rd); its move north was to be concealed by deception. The movement plan is shown overleaf; actual times were one or two days later. Inoperable and destroyed tanks, along with dummy tanks and SP assault guns made from wood and earth, were left in vacated positions. Army and Corps command posts continued radio transmissions. As 3 GTA moved north, units in the Bukrin area continued their "normal" activities. Artillery fired in the usual pattern, units strengthened their positions and conducted recce. Rumours were planted of a new offensive, which involved the refitting of 3 GTA and the billeting of new tank units East of Kiev. In support of this rumour campaign, rifle bns with tanks conducted exercises in the Bukrin bridgehead, while false traffic movements continued to and fro across the river. Within the bridgehead rear service units constructed mock-up huts and dugouts, complete with

smoke. At night, bonfires were lit to simulate troop concentrations. Meanwhile, 38 Army around Lyutezh simulated the intent to launch limited attacks westward, rather than southward (where the real attack was to occur). To force the Germans to focus their efforts on the Bukrin area, the remaining Soviet forces attacked westwards on the day of the attack in the Lyutezh area

The Result

6. The deception was successful. Until 30 Oct the German maps showed 3 GTA in the Bukrin bridgehead. They then showed it outside the bridgehead, on the East side of the River Dnieper. It was not until 3 Nov that the Germans realised that 3 GTA was in the Lyutezh area, but they still held it on the East bank. By then it was too late as the Soviets launched their attack on that day. 3 GTA's attack came as a complete surprise to the defending Germans, and they were quickly overwhelmed.

Lessons from 3 GTA's Regrouping

7. The aim of the deception was simple: to cause the enemy to commit his reserves in the Bukrin area by portraying a credible threat in that area. It also demonstrates that a simple plan, using resources already at hand, can deliver the required result. The use of inoperable vehicles can deceive even the most sophisticated ISTAR systems; a tank with, say, a damaged gearbox looks identical to a fully functional one. The continuation of routine activity has been a feature of many deception plans and is not resource-intensive.

CHAPTER 4

EXAMPLES OF PARTICULAR TECHNIQUES

OPSEC

The Ardennes Offensive, Europe 1944

1. On 16 Dec 44, to the astonishment of the Allies, the German Army Group B, commanded by Field Marshal Model, totalling 28 Divisions, burst out of the heavily wooded and hilly Ardennes, taking the US VIII Corps completely by surprise. Preceded by heavy artillery bombardment, Panzer and *Volksgrenadier* divisions swept through the surprised Americans, with the objective of taking Antwerp and splitting the Allied forces. Operation WACHT AM RHEIN was ultimately defeated, but what is important is their achievement of total surprise against forces with state-of-the-art (for the period) ISTAR capabilities, and who were aware that some form of counterattack was likely at any time. The Germans achieved their surprise through a security plan which addressed all aspects of the operation, identifying those indicators of the operation that the Allies would be looking for, and providing them with the appropriate security.
2. Any major military operation needs reinforcements and reserves. During the preparatory phase of Op WACHT AM RHEIN, a basic principle of the deployment of reserve formations was that on no account was the enemy to draw the conclusion from their dispositions that an offensive might be contemplated. A deception plan was implemented, but this was not central to the security plan. Formations were given camouflage designations to conceal their identities, and a fictitious 25th Army was created near Cologne to draw the Allies' attention. There is no record that this had any real impact on the Allies' perception of events. Instructions were given on action to be taken in the event of betrayals by deserters, and on the capture of reconnaissance patrols and combat outposts. Particularly stressed was the importance of reporting any sign that the enemy was growing suspicious. During the development of the plan of attack, the overall picture of the plan was scarcely mentioned, Model confining his explanations to essential matters. The offensive was even given a new name (HERBSTNABEL) in Dec 44.
3. Formations moving forward to take their positions for the attack were forbidden to advance past a line into the area where there was a risk of the Americans prematurely taking prisoners. The Germans were largely dependent on EW, and reconnaissance and combat patrols, for their intelligence. It was forbidden to intensify the efforts of the latter. These patrols were also tasked with identifying signs of unusual activity on their own side as seen from forward allied positions. At the end of Nov 44, patrol activity was stopped to avoid compromise should any be taken prisoner.
4. The "need to know" principle was strictly enforced, with each level of command only knowing about their own part in the plan. Personnel whose commitment to the cause might be considered suspect, ie soldiers originating from Alsace, Lorraine or Luxembourg, were not sent to the forward area. Routine countersurveillance procedures were enforced at all times, such as movement by night and camouflage discipline.

5. A vital point, which contributed much to the success of the security plan, was that it addressed the operation as a whole and was co-ordinated at the highest level. Security measures were examined, and their effectiveness monitored, from an enemy viewpoint. The end result of these measures and precautions was complete surprise.
6. The Allies began their counterattack in early Jan 45, and by the 28th had recovered all the ground lost in December. The German offensive was over-ambitious and was a desperate last gamble to defeat the Allies in the West. However, its eventual failure does not distract from its earlier successes. As an indication of the sheer scale of the security plan, some 20 divisions were moved into the attack area without arousing Allied suspicions.

Dien Bien Phu, 1953-4

7. In November 1953 the French in Indo-China (Vietnam) established a large force at Dien Bien Phu, 125 miles from Hanoi. Its aim was to draw General Giap's Viet Minh forces into a large-scale conventional battle where they could be destroyed. The French forces relied heavily upon their assumed air and artillery superiority. Giap, in fact, had received over two hundred 75 and 105 mm guns and a large quantity of AA weapons from the Soviets. This enhanced capability, which was obtained covertly, was critical to his strategy of encouraging the French to pour more men into what would become a huge killing zone, whose only effective means of resupply was by air.
8. Over the next four months Giap moved his artillery from bases on the Chinese border under conditions of strict control and complete secrecy. Guns and ammunition were carried by relays of porters, using trails beneath the jungle canopy and cover of night. Although there were intelligence reports of some activity, the French higher command were unaware of the size and scale of Giap's artillery. On 13 Mar 54, the Viet Minh began the battle in earnest with a massive artillery bombardment. French resupply was rendered almost impossible by a combination of AA fire and artillery strikes on the airhead. After almost 2 months of fighting the French were forced to surrender on 8 May 54 with the loss of almost 12,000 men. OPSEC made a major contribution to the Viet Minh victory. Although the French were aware that the Viet Minh were present in large numbers, and that an offensive was planned (although the French intended this), they remained unaware of critical enemy activities and capabilities until too late.

DECEPTION

Marlborough's March to the Danube

9. In 1704, during the War of Spanish Succession, Marlborough, then in Holland, needed to reach Bavaria (France's ally) before the French, in order to prevent them linking up. He gained a start on the French by moving so fast that they were unable to react in time. To maintain his lead, he used deception. Marlborough marched up the Rhine towards Phillipsburg, where the French expected him to cross the Rhine in order to attack Alsace. Marlborough had a bridge of boats prepared at Phillipsburg, appar-

ently confirming his intention to cross. On his arrival there, however, he continued up the Rhine towards the Danube. By the time the French realised what was happening, Marlborough had gained the vital lead he needed to link with his German allies and take on the Bavarians. This campaign ended with Marlborough's victory at Blenheim.

10. Marlborough's deception was a combination of the obvious solution (he was expected to cross the Rhine and attack France) and manoeuvre (he moved faster than his enemy). This deception used few resources; enough men and materials to build a simple boat bridge. His aim was not to use deception to win a battle there and then, but simply to gain a time advantage over his enemy, allowing him to maintain the initiative and control events. With today's fast-moving battles, gaining even a few minutes on an enemy could give a commander a critical edge.

Yom Kippur, Oct 1973

11. Following their defeat by the Israelis in the Six Day War of 1967, the Egyptians were pushed back to the West Bank of the Suez Canal. This formidable obstacle, which was under continuous surveillance by Israeli forces, had to be crossed to regain any Egyptian territory in the Sinai. The open desert terrain and the large forces needed to attempt a crossing precluded any attempt at surprise through concealment. A long-term deception plan was therefore implemented; details of which were known only to a few senior Egyptian officers.
12. From autumn 1972 onwards, the Egyptians conducted about 40 major obstacle crossing exercises on the Nile and other canals in Egypt. Training on new Soviet equipment was carried out. This training was expected by the Israelis, and seen as routine. Several mobilisation exercises were held, with men being called up and then released in an irregular sequence. This made it virtually impossible to gauge the strength of the Egyptian forces at any one time. The Egyptians held exercises on the West bank of the Suez Canal, bringing large quantities of bridging equipment and other stores. This was seen to be removed on completion of the exercises but, unbeknown to the Israelis, some was left behind each time in underground stores.
13. The constant presence of Egyptian troops (often seen off-duty and bathing in the Canal) and equipment, coupled with the lack of any obvious preparations for war, lulled the Israelis into a false sense of security. Routine leave and courses continued among the Egyptian troops. COMSEC, a vital element of OPSEC, was excellent and, where possible, the Egyptians used landline. Although the Israelis became suspicious in early October, their government decided to take no action. When the attack came on 6 Oct 73, the Israelis were taken by complete surprise and the Egyptians crossed the Canal with minimal losses. Egyptian security was so tight that on the morning of the attack, only 2% of their junior officers were aware that they were not participating in yet another exercise.
14. This was a strategic deception, but lessons can be drawn that apply at lower levels. The technique of the false routine can be used at any level, and has considerable potential in OOTW. It also shows that selection of deception target is critical; in this case, the deception was ultimately aimed not at the opposing military commander, but at those with the appropriate influence, ie the Israeli government.

Falklands Islands, May 1982

15. The Argentinean attack on the Falkland Islands came as a surprise to the UK government. The necessary speed of their response did not allow time for a strategic deception, and the resultant Task Force's goal was impossible to disguise. The tactical deception measures were centred on drawing the enemy's attention away from the intended landing areas. Covert reconnaissance on potential landing sites was conducted, and air and artillery preparation was carried out in four coastal areas. An actual landing was conducted in one area, with demonstrations in the other three.
16. The chosen landing area was San Carlos Water. The Argentineans decided that the main landing would be in the Port Stanley area, where naval and air harassment had been concentrated. The Assault Group sailed towards Port Stanley on 20 May 82, confirming this assessment. When they were just below the horizon, the Assault Group altered course westwards and made the final approach to San Carlos in the dark. Naval bombardments were directed at three other sites, and the SAS made a noisy diversion at Darwin. When the beachhead was established the following day, the Argentineans assumed that it was a diversion, which gave a few more hours before they began to counter-attack in strength.
17. The Argentineans were not the only ones being deceived. Post-attack aerial photography of RAF bombing of Port Stanley airfield revealed apparent heavy damage of the runway. It was subsequently learnt that many of the "bomb craters" on the runway were created by the Argentineans, using loose earth on an otherwise undamaged surface to make realistic crater rims. These were then cleared at night to allow resupply aircraft to land.
18. The Falklands shows that it is possible to conduct effective deception operations with short lead times and few resources. In this case, tactical deception measures were used to further operational goals.